

1 JOHN S. LEONARDO  
United States Attorney  
District of Arizona

2  
3 FREDERICK A. BATTISTA  
Maryland State Bar Member  
PETER S. SEXTON  
Arizona State Bar No. 011089  
4 JAMES R. KNAPP  
Arizona State Bar No. 021166  
Assistant U.S. Attorneys  
5 Two Renaissance Square  
40 North First Avenue, Suite 1200  
6 Phoenix, Arizona 85004  
Telephone: (602) 514-7500  
Fred.Battista@usdoj.gov  
7 Peter.Sexton@usdoj.gov  
James.Knapp2@usdoj.gov

8 UNITED STATES DISTRICT COURT  
9 DISTRICT OF ARIZONA

10 United States of America,  
11  
12 Plaintiff,  
13  
14 v.  
15 Daniel David Rigmaiden,  
Defendant.

No. CR-08-0814-001-PHX-DGC  
**GOVERNMENT'S RESPONSE TO  
DEFENDANT'S MOTION TO  
SUPPRESS**

16 The United States, through undersigned counsel, opposes defendant's motion to suppress.  
17 (CR 824.) As argued below, the United States' collection of historical records pursuant to  
18 subpoenas and court orders was reasonable, the FBI's efforts to locate the aircard pursuant to  
19 the tracking warrant were reasonable, and the search of defendant's apartment and computer  
20 pursuant to the search warrant was reasonable. Accordingly, his motion should be denied.

21 Defendant's brief contains nearly 200 pages of alleged facts and more than 150 pages of  
22 argument, along with two addenda with 20 pages of additional arguments. The motion also  
23 includes four lengthy declarations from defendant and references thousands of pages of proposed  
24 exhibits. Other pleadings have also been filed by defendant regarding the seizure of evidence  
25 in this case. In total, CR 824, 826, 830, 847, 857 and 858. Rather than respond point by point  
26 to these pleadings and materials, which seems certain to result in more voluminous filings, the  
27 United States has attempted to address defendant's arguments by grouping them into categories.  
28 No doubt some allegations have been left unanswered. This is not a concession that they are true

1 or legitimate; to the contrary, it is a conclusion that they are irrelevant. The United States will  
2 provide supplemental briefing on any of defendant's allegations or claims, however, upon the  
3 Court's request.

4 **I. Statement of Facts.**

5 Defendant was a thief and a fugitive. Known only as "the Hacker" to his co-conspirators  
6 and the federal agents who pursued him, defendant stole hundreds of identities, compromised  
7 numerous innocent victims' computers, compromised numerous other innocent victims' financial  
8 affairs, filed more than 1,200 fraudulent tax returns with the Internal Revenue Service and  
9 laundered hundreds of thousands of dollars through co-conspirators' bank accounts.<sup>1/</sup>

10 1. Overview of the Scheme

11 The investigation that led to the arrest of defendant Daniel David Rigmaiden was a joint  
12 investigation involving the Internal Revenue Service - Criminal Investigation (IRS-CI), the  
13 Federal Bureau of Investigation (FBI), and the U.S. Postal Inspection Service (USPIS). The  
14 investigation initially led to the authorization of a Northern District of California Search Warrant  
15 No. 08-70460-HRL, on July 22, 2008. The authorization required that the warrant be executed  
16 within 10 days. Due to the fact that the occupant of the subject apartment had not been observed  
17 in the area, the warrant was not executed and was returned not executed on July 30, 2008. On  
18 that same date, upon an independent finding of probable cause, the investigation team obtained  
19 Northern District of California Amended Search Warrant No. 08-70460-HRL (hereinafter SW  
20 08-70460) (CR 464-2), and executed the amended warrant at defendant's apartment on August  
21 3, 2008. The execution of the warrant revealed significant evidence related to a sophisticated  
22 scheme to fraudulently obtain tax proceeds filed in the name of innocent third parties and  
23 deceased individuals, and illegally obtain the proceeds from these tax returns. Up until  
24 defendant's arrest and identification through fingerprint analysis, he was primarily known to the  
25 investigation team and his associates who had agreed to cooperate against him simply as the

---

26 <sup>1/</sup> There is no known evidence that defendant ever personally referred to himself at the  
27 "Hacker."  
28

1 “Hacker.” Through their efforts, the investigation team determined that the Hacker operated in  
2 the United States, was involved in acquiring identity information of deceased and living  
3 individuals, including their social security numbers, and using that information to conduct an  
4 electronic bulk tax filing scheme; and directing the deposit of the proceeds of those fraudulent  
5 tax returns to bank accounts and debit cards where the funds could be accessed by the Hacker  
6 and co-conspirators.

7 Prior to the authorization of SW 08-70460, the investigation team determined that for tax  
8 year 2006, refunds totaling approximately \$1,112,040.00 were falsely claimed via the subject  
9 electronically filed returns. Based on the significant similarities associated with the IP  
10 addresses, return format, and e-mail addresses, the IRS Fraud Detection Center located in  
11 Austin, Texas (AFDC) identified approximately 1,272 returns, 175 IP addresses, and 73 bank  
12 accounts that were believed to be linked to this scheme for tax year 2007. As of June 26, 2008,  
13 refunds totaling approximately \$2,133,824.00 had been falsely claimed via electronically filed  
14 returns for the 2007 tax year.

## 15 2. Carter Tax and Accounting – The Tip of the Iceberg

16 In May 2007, IRS-CI in Phoenix became aware of questionable activity involving an  
17 account in the name of Carter Tax & Accounting LLC. Subsequent co-defendant Ransom  
18 Marion Carter was the authorized signer for the account. Between May 22 and May 25, 2007,  
19 75 U. S. Treasury electronic credits totaling approximately \$129,364.00 labeled “tax refund”  
20 were posted to the account. On May 26, 2007, Ransom Carter withdrew \$24,500.00 from the  
21 account and purchased two cashier’s checks with the funds.

22 On June 5, 2007, EFile Tax Returns, Inc., an authorized IRS e-file provider and member  
23 of the Free File Alliance LLC, contacted the ETA, regarding a large volume of returns filed  
24 through its website using what appeared to be an automated process. EFile Tax Returns, Inc.,  
25 identified approximately 200 returns for tax year 2006 and 400 for tax year 2005, which  
26 appeared to be related to the subject automated scheme.

1 The AFDC researched the returns identified by EFile Tax Returns, Inc., and identified  
2 Ransom Carters' Compass Bank account as one of the accounts destined to receive refunds  
3 claimed on those returns. A search was conducted for all electronically filed returns with  
4 refunds destined for the above referenced Compass Bank account. Approximately 209 returns,  
5 claiming over \$339,000.00 in refunds, were identified bearing this particular bank account  
6 number and routing number.

7 IRS-CI analysis of the subject returns revealed multiple fraudulent returns filed from  
8 single IP addresses within short time periods, indicating the use of some type of computerized  
9 bulk filing system. Based on analysis of the IP addresses, it appeared the returns were filed from  
10 multiple locations around the United States. However, the real IP address was apparently  
11 hidden, possibly by utilizing illicit proxies or intermediary computers to submit the returns and  
12 prevent the identification of the individual filing the returns.

13 3. Informants CI 1 and CI 2 Who Lead the Investigation Team to the Hacker

14 In January 2008, an individual pending unrelated felony fraud charges, in the Superior  
15 Court of Arizona, agreed to provide information to IRS-CI and USPIS in order to potentially  
16 gain consideration with respect to his/her pending state charges. This individual will hereinafter  
17 be referred to as CI 1. As of the date of the authorization of SW 08-70460, based on information  
18 known to IRS-CI, CI 1 was believed to be credible and his/her information had been  
19 corroborated and documented through independent investigation, recorded telephone calls, and  
20 recorded e-mails. In a debriefing, CI 1 advised that an individual he/she knew only by his/her  
21 street name (initially SN 1 in the affidavit and then CI 2) and another unknown individual CI 1  
22 referred to as the Hacker, had been operating an automated system to file fraudulent tax returns  
23 using the names and Social Security Numbers of deceased individuals.

24 CI 1 further stated Ransom Carter's receipt of refunds through the Compass Bank account  
25 Carter established in 2006, in the name of Carter Tax & Accounting LLC, represented a  
26 successful test run of the scheme. CI 1 said SN 1 and his associates intended to pursue the same  
27 scheme for the 2008 filing season (for income earned in 2007). CI 1 also stated he/she believed  
28

1 that during prior years, going back as far as 2005, the fraudulent tax returns had directed refunds  
2 be credited to pre-paid debit cards.

3 Based on the information provided by CI 1 and CI 1's agreement to work as a confidential  
4 informant on behalf of law enforcement, an undercover operation was initiated by IRS-CI and  
5 USPIS to determine the true identity of SN 1, the Hacker and their associates, and gather  
6 evidence concerning the nature and extent of the bulk filing scheme. Per SN 1's instructions to  
7 CI 1, IRS-CI and USPIS, with the assistance of CI 1, established an undercover shell business  
8 and a related undercover bank account at Meridian Bank ("Meridian undercover bank account").

9 In the course of the scheme, SN 1 asked CI 1 to open a safe mail.net e-mail account. The  
10 purported purpose of using this e-mail service was to avoid detection. In February 2008, CI 1  
11 e-mailed the account number and routing numbers for the Meridian undercover bank account  
12 to SN 1. SN 1 subsequently advised CI 1 the Hacker would begin to e-file fraudulent returns  
13 which directed refunds be sent to the Meridian undercover bank account. Throughout the initial  
14 stages of the undercover operation, CI 1 communicated with SN 1 via telephone and his safe  
15 mail.net account. Incoming e-mails from SN 1 revealed a particular IP address which an internet  
16 directory service revealed is owned by Comcast Cable Communications, Inc. In late February  
17 2008, in response to a Grand Jury subpoena, Comcast reported the subject IP address was leased  
18 by SN 1 at SN 1's residential address. It was determined SN 1 was, in fact, the subscriber.

19 In early March 2008, the AFDC identified 72 electronically filed tax returns with refunds,  
20 totaling approximately \$117,496.00, destined for the Meridian controlled undercover bank  
21 account. Over \$62,000.00 was deposited to the Meridian undercover bank account in  
22 mid-March 2008. After the aforementioned deposits, CI 1 contacted SN 1 and informed him  
23 money had been deposited in the account. CI 1 told SN 1 he/she would withdraw \$9,000.00 in  
24 mid-March 2008 and ship it to SN 1 on March 18, 2008, via FedEx. CI 1 further advised he/she  
25 would withdraw money from the account every week and ship \$9,000.00 to SN 1 every other  
26 week. The withdrawn money not "shipped" was to be CI 1's cut. SN 1 provided CI 1 with the

1 name and address where the money was to be shipped. SN 1 also told CI 1 to provide the  
2 tracking number so he could monitor the shipment of the package.

3 In late March 2008, an IRS-CI agent withdrew \$9,000.00 in currency from the Meridian  
4 undercover bank account and on April 1, 2008, \$9,000.00 was shipped overnight priority mail  
5 to SN 1. For the first and second shipments, agents witnessed SN 1 leave his/her personal  
6 residence, arrive at the destination of the package delivery, leave the destination with a package  
7 appearing to be the undercover package, and return to his/her residence.

8 On April 14, 2008, a third shipment in the amount of \$9,000.00 currency was sent  
9 overnight priority mail to SN 1. On April 15, 2008, SN 1 was arrested when leaving the  
10 destination location carrying the third and final shipment of \$9,000.00 currency.

11 After his/her arrest on related federal charges, SN 1 agreed to act as a confidential  
12 informant and assist law enforcement in identifying and apprehending the Hacker and will be  
13 hereinafter referred to as CI 2. CI 2 then advised he/she had never met the Hacker in person and  
14 had never spoken to the Hacker telephonically or via Voice Over Internet Protocol (VOIP). CI  
15 2 maintained ongoing contact with the Hacker via encrypted e-mail using a safe-mail.net e-mail  
16 account. Safe-mail.net is located in the country of Israel. CI 2 has also indicated the Hacker  
17 previously operated a website (www.fakeid.tv) where the Hacker sold fake California driver's  
18 licenses.

19 4. The Controlled Delivery of \$68,000.00 to the Hacker

20 The Hacker had been led to believe CI 2 had an associate, "Daniel," who worked in the  
21 banking industry and was willing to assist CI 2 in moving the "Hacker's" fraudulent tax return  
22 proceeds from the Meridian undercover bank account quickly and without detection.

23 On April 17, 2008, CI 2 sent an encrypted e-mail to the Hacker explaining he/she had  
24 received an additional \$9,000.00 in currency from the Meridian undercover bank account, and  
25 was expecting to receive an additional \$75,000.00 by April 22, 2008. CI 2 inquired how the  
26 Hacker wanted his cut (\$68,000.00) of the money. The Hacker provided CI 2 detailed  
27 instructions regarding how to physically wash \$68,000.00 in currency in lantern fuel to remove  
28

1 any drug or explosive residues which might cause a detection dog to alert on the package. CI  
2 2 was further instructed to double vacuum seal the currency, to place the sealed currency in the  
3 cavity of a toy, gift wrap the toy so it appeared to be a present, attach a birthday card for a dying  
4 child, package it for overnight FedEx delivery, and have the package held for pickup at the  
5 destination location.

6 Additionally, the Hacker informed CI 2 he would send a courier, armed with an AR-15  
7 in a duffle bag, to pick up the package. The Hacker added the courier would be prepared to  
8 shoot anyone who attempted to arrest him while he was in possession of the package. The  
9 Hacker informed CI 2 he would send details of the operation in an encrypted format to the media  
10 before the pickup date. If law enforcement conducted a sting on the pickup, the Hacker would  
11 then provide information to the media to decrypt his prior message. The Hacker advised this  
12 would make law enforcement look bad by proving that law enforcement knew the potential for  
13 violence at a public place before conducting the sting.

14 On May 5, 2008, the Hacker sent CI 2 an encrypted e-mail with directions to send a  
15 package containing \$68,000.00 in currency to Patrick Stout, to a commercial address in Palo  
16 Alto, California, and to arrive the morning of May 6, 2008. This location was determined to be  
17 a FedEx/Kinko's retail store open 24 hours a day. Prior to the shipment, CI 2 provided the  
18 Hacker with the undercover package's tracking number via another encrypted e-mail.

19 The package containing \$68,000.00 in currency was delivered to the FedEx/Kinko's store  
20 on May 6, 2008. On May 7, 2008, at approximately 5:00 am, a then unknown white male,  
21 average build, wearing a dark jacket with a hood, who appeared to be in his twenties and  
22 presented identification in the name "Patrick Stout," was observed entering the back entrance  
23 of the Fed Ex/Kinko's on foot and retrieving the package. The male carried the box to a nearby  
24 corner where he ripped open the box, removed the contents containing the currency and  
25 discarded the packaging in a nearby dumpster. The then unknown male proceeded toward a  
26 nearby train station. Agents conducting surveillance were unsuccessful in efforts to identify the  
27 then unknown male or follow him to his final destination. Upon execution of SW 08-70460,  
28



1 identification bearing defendant's photograph and the false identity "Patrick Stout" was found  
2 in defendant's apartment along with many of the pre-recorded \$100 bills that were part of the  
3 \$68,000 shipment.

4 On or about May 8, 2008, the Hacker e-mailed CI 2 and confirmed receipt of the money.  
5 The Hacker indicated in his e-mail the money was picked up by a third party. The Hacker  
6 advised CI 2 that the courier who retrieved the package believed that he was being followed by  
7 police. According to the Hacker, the courier advised he noticed a "car circling around the area  
8 after he left with the driver acting like he was looking for someone. There were also some  
9 suspect characters walking around on foot 'trying to follow him' so he said he did a 180 and  
10 'came right at them' but they did not do anything about it. The Hacker then advised that the  
11 courier was "likely just really paranoid."

12 5. False Identity No. 1 for the Hacker - "Patrick Stout"

13 Investigation of the name "Patrick Stout" led the investigation team to a Post Office Box  
14 located in Sacramento, California, that was opened under the name "Patrick Stout" on November  
15 21, 2007 and was closed on May 31, 2008. Investigation of the information provided to open  
16 the Post Office Box determined that the California Driver's License number used to open the  
17 Post Office Box was actually assigned to a female with a different name in California.

18 Approximately two weeks after the "Hacker's" receipt of the \$68,000 controlled delivery,  
19 an account was opened with Bullion Direct in the name of "Patrick Stout." According to its  
20 website prior to the authorization of SW 09-70460, Bullion Direct held itself out to be an online  
21 source to buy and sell precious metals, including gold, silver, platinum and palladium coins and  
22 bars. Bullion Direct shipped precious metals to customers via UPS/FedEx or United States  
23 Postal Service registered mail. The investigation further revealed that an unknown individual  
24 used a debit card, which was linked to fraudulent tax refunds, to purchase United States Postal  
25 Money Orders. The postal money orders were then used to purchase gold through Bullion Direct  
26 for the "Patrick Stout" account. Two separate shipments of gold, totaling approximately  
27  
28



1 \$18,000, were mailed via FedEx to “Patrick Stout”, to the same FedEx/Kinkos location as the  
2 \$68,000 controlled delivery.

3 6. The Bigger and Better “Daniel” Undercover Account

4 After the \$68,000 controlled delivery, CI 2 and the Hacker soon thereafter agreed  
5 “Daniel” would withdraw all of the money from the Meridian undercover bank account and  
6 deposit the money in an account controlled by “Daniel.” CI 2 informed the Hacker, “Daniel”  
7 was able to make very large one-time withdrawals only at the end of each quarter, the next  
8 quarter ending June 30, 2008.

9 On May 16, 2008, CI 2 informed the Hacker that “Daniel” had moved \$364,260 (the  
10 remaining cut for CI 2 and the Hacker) from the Meridian undercover bank account into another  
11 bank account believed to be controlled by “Daniel.” CI 2 provided a Bank of America routing  
12 number and undercover account number to the Hacker where future tax refunds could be  
13 deposited. Per the Hacker’s request, the funds in the Bank of America account would be swept  
14 weekly into another account controlled by “Daniel.”

15 On May, 27, 2008, the Hacker informed CI 2 he had filed approximately 200 additional  
16 fraudulent tax returns seeking refunds destined for the new undercover account located at Bank  
17 of America. As of June 26, 2008, the AFDC had identified 249 fraudulent tax returns claiming  
18 approximately \$404,382 destined for this account. The returns were filed from multiple IP  
19 addresses.

20 7. False Identity No. 2 - “Travis Rupard”

21 On March 1, 2008, a fraudulent tax return for James A. Johnson (xxx-xx-3549) was filed  
22 with the Internal Revenue Service using IP address 75.208.105.186, with a refund amount of  
23 \$2,099.00 destined for a debit card issued by Galileo Processing. This debit card account was  
24 linked by the investigation team to the Meridian undercover bank account through analysis of  
25 connected IP addresses and bank accounts. The account holder was listed as James Johnson  
26 (xxx-xx-8024) with an address in Alameda, California. The AFDC identified additional tax  
27 returns electronically filed claiming refunds destined for same account as follows:

Date	Name	Social Sec #	City, State	Refund	IP Address
01/19/08	James L Johnson	xxx-xx-5366	Culver City, CA	\$2,397	24.205.80.123
02/07/08	James Johnson	xxx-xx-4889	Bentonville, AR	\$2,437	76.195.145.182
02/29/08	James B Johnson	xxx-xx-1692	Rocky Ridge, MD	\$717	67.82.193.84
02/29/08	James B Johnson	xxx-xx-8023	Culver City, CA	\$1,384	76.250.136.120
03/01/08	James D Johnson	xxx-xx-7537	North Wilkesboro, NC	\$2,249	68.36.156.35
03/01/08	James C Johnson	xxx-xx-4542	Chicago, IL	\$1,061	68.36.156.35

On March 1, 2008, a fraudulent tax return for Michael S. Deshields (xxx-xx-8782) was filed with the Internal Revenue Service using IP address 75.208.105.186, with a refund amount of \$1,988.00 destined for a debit card issued by NetSpend. This debit card account was linked by the investigation team to the Meridian undercover bank account through analysis of connected IP addresses and bank accounts. The account holder was listed as Barbara L. Piper (xxx-xx-8344) with an address in Detroit, Michigan. The AFDC identified three additional tax returns electronically filed claiming refunds destined for the same debit card account as follows:

Date	Name	Social Sec #	City, State	Refund	IP Address
01/22/08	Barbara Piper	xxx-xx-8344	Marion, IN	\$5,514	24.251.75.193
02/29/08	Arjuna Desilva	xxx-xx-6629	Phoenix, AZ	\$1,463	208.97.32.251
02/29/08	Banhdasack Detsadachanh	xxx-xx-5124	Lake Havasu City, AZ	\$1,861	68.36.156.35

On March 5, 2008, a tax return for Robert W. Galletly (xxx-xx-7628) was filed with the Internal Revenue Service using IP address 75.209.41.104, with a refund amount of \$1,093.00 destined for a debit card issued by Account Now. This debit card account was linked by the investigation team to the Meridian undercover bank account through analysis of connected IP addresses and bank accounts. The account holder was listed as Margaret Murray (xxx-xx-0901)

with an address in Petersburg, Virginia. The AFDC identified three additional tax returns electronically filed claiming refunds destined for the same debit account number as follows:

Date	Name	Social Sec #	City, State	Refund	IP Address
01/17/08	Margaret Murray	xxx-xx-0901	Millville, NJ	\$3,907	68.44.96.153
03/05/08	Beth A Gallamore	xxx-xx-5092	Phoenix, AZ	\$1,490	99.130.28.126
03/25/08	Justin P Hopper	xxx-xx-9313	West Chester, PA	\$980	24.61.51.52

On March 26, 2008, a tax return for Kevin Furman (xxx-xx-8975) from Eugene, Oregon, was filed with the Internal Revenue Service using IP address 75.209.101.132, with a refund amount of \$1,282.00 destined for the Meridian undercover bank account. Furman died on August 30, 1989.

Investigation revealed the IP addresses associated with the James Johnson, Michael Deshields, Robert Galletly, and Kevin Furman tax returns were registered to Verizon Wireless. In response to a Federal Grand Jury subpoena, Verizon Wireless reported that IP addresses 75.208.105.186, 75.209.41.104, and 75.209.101.132 were utilized by a person who opened the account in the name of Travis Rupard, with Post Office Box 730031, San Jose, California, and telephone number (206) 666-3620. The above mentioned IP addresses were linked via the following mobile device number (MDN): (415) 264-9596. Verizon Wireless issued the Broadband Access Card to Travis Rupard, with ESN 005-00717190, assigned telephone number (415) 264-9596 and Verizon Wireless account number 270691733, to the customer claiming to be "Travis Rupard" on May 23, 2006. This device will hereinafter be referred to as the "Aircard."

USPIS conducted an investigation of Post Office Box 730031 in San Jose, California and determined this PO Box was opened on March 31, 2006 and was closed on August 31, 2006. The application indicated an individual purporting to be Travis Rupard presented a California Driver's License, number D2740168 and a Student ID Card, and provided a physical address of 1780 Oakland Road, #17, San Jose, California, 95131. Further investigation showed the

1 California Driver's License number was assigned to a female with a Bakersfield, California,  
2 address. Based on information provided by the San Jose, California, Post Office, the address  
3 1780 Oakland Road was a physical street address for the Leasing Offices of an apartment  
4 complex in San Jose. There were no apartment numbers or suite numbers associated with 1780  
5 Oakland Road, San Jose, California.

6 8. False Identity No. 3 - "Aaron Johnson"

7 CI 2 advised that he/she had been involved with the Hacker in a number of fraudulent  
8 schemes over a period of several years and in the past he/she had sent money to the Hacker by  
9 sending it to e-gold account XXXX337. A Federal Grand Jury subpoena was issued for  
10 documents related to this account. Records showed that this account was created on August 16,  
11 2006, in the name of Sam Blat and Benjamin Cohan. Records corroborated that CI 2 sent the  
12 Hacker \$7,640 on August 17, 2006. The Sam Blat account sent money to an account in the  
13 name of Aaron Johnson on five occasions beginning on November 19, 2006 through December  
14 22, 2006. On July 31, 2006, an account in the name of Travis Rupard, 6447 Ivy Lane, San Jose,  
15 California, 95129, e-mail address travisrupard@safe-mail.net, telephone number (408)  
16 252-1678, sent \$9.50 to the Aaron Johnson account. The name Aaron Johnson was listed as the  
17 account holder of a Southwest Bank Account used to receive fraudulent tax refunds. In the  
18 course of the undercover investigation, the Hacker asked CI 2 to inquire about the Southwest  
19 Bank Account with "Daniel" to determine if the Hacker could obtain proceeds in the account.  
20 The Hacker had advised CI 2 that he had been unable to withdraw the proceeds from the scheme  
21 out of this account.

22 9. The Role Played by Time Zones in the Investigation, IP Transaction Records for  
23 the Hacker & CI 2 E-mails

24 On or about June 25, 2008, in response to an Order issued pursuant to 18 U.S.C. §  
25 2703(d), Verizon Wireless provided IP transaction information related to the IP addresses  
26 utilized by the Verizon Travis Rupard account identified above. Verizon Wireless reported  
27 connection times in Greenwich Mean Time (GMT). GMT was researched on  
28 www.greenwichmeantime.com. The website indicated that during Daylight Saving Time (DST),



the successful logon to the Meridian undercover bank account by IP address 81.27.4.177. Verizon Wireless broadband access card connection records (obtained pursuant to an Order issued pursuant to 18 U.S.C. 2703(d)) reported the Travis Rupard Account connected to IP address 81.27.4.177 multiple times on May 16, 2008 including connections during 12:42 p.m. 12:43 p.m. and 12:44 p.m. GMT.

On May 24, 2008, the Hacker attempted to logon to the Meridian undercover bank account from IP address 68.199.62.250. At 11:00:02 Arizona time, the bank rejected the logon because the computer was not recognized and challenged the user. At 11:01:34, Arizona Time, after entering the one time security code and enrolling the computer, the Hacker's login was authenticated. The Hacker accessed Account Summary, Account History and a Check Image.

On May 24, 2008, at 06:00:36 p.m. GMT, IP address 68.199.62.250 accessed the e-mail account andersonsats@gmail.com. This e-mail access was after the logon rejection yet before the successful logon to the Meridian undercover bank account by IP address 68.199.62.250.

Verizon Wireless broadband access card connection records (obtained pursuant to an Order issued pursuant to 18 U.S.C. 2703(d)) reported the Travis Rupard Account connected to IP address 68.199.62.250 multiple times on May 24, 2008, including connections during 6:00 p.m., 6:01 p.m. and 6:02 p.m. GMT.

#### 11. Analysis of IP Addresses Used to File Fraudulent Tax Returns

The IP Addresses logged for the 395 tax returns filed using the undercover bank account located at Meridian Bank were researched on an internet reference directory. A sampling of the IP addresses and ISP information is set forth below:

IP Address	Internet Service Provider	No. of Returns	Subscriber	City & State
12.216.17.121	Media Com Communications	10	Janet Martin	Des Moines, IA
24.26.218.97	Time Warner Cable	21	Bruce Hicks	Belton, TX
24.17.47.176	Comcast Cable Communications Inc.	9	Gayle Johnston	Willow Springs, IL

67.168.17.7	Comcast Cable Communications Inc.	18	Derek Smith	Federal Way, WA
67.175.211.144	Comcast Cable Communications Inc.	2	Valerie Wachholz	Mundelein, IL
75.209.101.132	Verizon Wireless	1	Travis Rupard	San Jose, CA

Based on the analysis of the IP Addresses, it appeared as if the returns were filed from multiple locations throughout the United States. However, due to the nature of the information contained in the returns, and the manner in which they were filed, it appeared the real IP Address, or IP Addresses, were hidden, possibly by use of IP spoofing, IP anonymizer services, or utilizing a botnet to submit the returns. In order to gain additional information regarding these types of activities, the affiant for SW 08-70460 consulted IRS-CI Special Agent Tracy Daun and FBI Special Agent Richard Murray. At that time, Special Agent Daun had been a special agent with IRS-CI since February 2001. She had participated in numerous criminal investigations relating to financial crimes, including but not limited to, income tax related crimes, money laundering, wire fraud, telemarketing fraud and mail fraud. Special Agent Daun expanded her expertise to include computer forensics, and computer crime scene investigations in January 2006, when she received training as a Computer Investigative Specialist (CIS) at the Federal Law Enforcement Training Center. She was trained in the execution of search warrants involving computers and related equipment, electronic data preservation, and the recovery, documentation and authentication of evidence. Special Agent Daun had taken computer related courses covering databases, spreadsheets, word processors, and other specialized software developed to assist with forensic analysis of digital data, digital evidence recovery, password detection, etc.

At that same time, Special Agent Murray had been an FBI Special Agent since 1999 and had been assigned to the Phoenix FBI Cyber Squad since 2005. SA Murray had participated in investigations relating to computer crime including computer intrusions and fraud committed using computers. SA Murray had received over 350 hours of computer crime training including,



1 but not limited to topics on Internet investigations, networking, computer intrusion  
2 investigations, computer security and wireless technology.

3 Special Agents Daun and Murray advised the affiant that using a proxy or intermediary  
4 computer could allow individuals to mask their true IP address and true identity and appear to  
5 be another computer. By using a proxy computer, an attacker could make it appear that his  
6 transmittal has come from another machine by sending and receiving communications through  
7 the proxy computer. In addition, they advised that IP anonymizer services are internet based  
8 anonymization tools available to hide an individual's real identity. An Internet user may visit  
9 an anonymizer tool's website and complete all of their web browsing/actions through the site.  
10 Special Agent Daun was aware of multiple free anonymizing websites on the internet including  
11 Anonymouse, iphide.com, and Proxify.

12 Special Agents Daun and Murray further advised that the term botnet was generally used  
13 to refer to a collection of compromised computers (called zombie computers) running programs,  
14 under a common command and control infrastructure. A botnet's originator could control the  
15 group remotely. A botnet typically ran hidden. While most owners are oblivious to the  
16 infection, the networks of botnets are frequently used to launch spam e-mail campaigns,  
17 denial-of-service attacks or on-line fraud schemes.

18 12. Tax Return Filing Activity by the Aircard

19 The AFDC reported the following fraudulent returns were filed on May 22, 2008, using  
20 IP address 24.3.79.57, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
19:38:01	JESSLYN ACERET	\$560.00
19:41:36	RICHARD R AUILERA	\$929.00
19:48:28	GINA M. ABAGNARO	\$1,538.00
19:57:27	MIGUEL A. ALARCON	\$1,566.00
20:00:12	DONALD M. ADAMS	\$1,756.00
20:11:55	KATRYNKA N. ADACHI	\$912.00
20:17:58	CHRISTOPHER B. AKIN	\$2,211.00

Verizon Wireless broadband access card connection records for the Travis Rupard account (obtained pursuant to an Order issued pursuant to 18 U.S.C. 2703(d)) showed connections to IP address 24.3.79.57 on May 23, 2008, as early as 12:29:43 a.m. GMT and as late as 7:00:41 p.m. GMT. Therefore, it appeared that the subject Aircard was used to file each of these fraudulent returns.

The AFDC reported the following fraudulent returns were filed on May 24, 2008, using IP address 24.47.154.61, with refunds destined for the undercover Bank of America account:

IP Time (PSDT)	Name	Refund Amount
13:28:07	STEVEN A. ABBOTT	\$2,150.00
13:30:56	MICHAEL Y. AHN	\$1,136.00
13:31:06	KEITH T. ALLEN	\$1,596.00
13:33:00	JOSEPH C. AIREY	\$1,006.00
13:42:12	ARTHUR A. ADOLPHSON	\$1,159.00
13:43:00	MICHAEL L. ADELMAN	\$479.00
13:44:07	DAVID C. ACKERMAN	\$1,303.00
13:44:55	ANA C. ALFARO	\$1,436.00
13:53:41	ELIZABETH ALLEN	\$1,857.00
13:58:03	CARLOS O. ALVARADO	\$507.00
14:00:25	RYAN D. ALVARADO	\$635.00
14:03:07	JAMES P. ACOSTA	\$2,179.00
14:05:51	CAROL S. AKINS	\$2,085.00
14:08:54	MIGUEL D. ADAME	\$1,034.00
14:09:52	MEMORIE P. AGUERRE	\$779.00
14:11:57	LARRY A. ACEVEZ	\$428.00
14:19:26	DAVID L. ALCANTAR	\$1,152.00
14:20:14	JOHN D. ADAMSON	\$1,930.00
14:21:17	MARIO C. ALONSO	\$602.00
14:25:35	DANIEL A. ACETO	\$953.00
14:30:45	DAVID R. ACUNA	\$655.00

Verizon Wireless broadband access card connection records for the Travis Rupard account (obtained pursuant to an Order issued pursuant to 18 U.S.C. 2703(d)) showed the Travis Rupard account with multiple connections to IP address 24.47.154.61 on May 24, 2008, as early as 8:23:51 p.m. GMT and as late as 9:30:59 p.m. GMT. Therefore, it appeared that the subject Aircard was used to file each of these fraudulent returns.

The AFDC reported the following fraudulent returns were filed on May 25, 2008, using IP address 74.73.116.37, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
12:11:53	DON A. ABELLA	\$1,945.00
12:17:18	ROGER L. ADAMS	\$1,329.00
12:23:41	REUBEN ALICEA	\$1,036.00
12:25:26	LUIS J. ALATRISTE	\$1,238.00
12:27:00	MICHAEL ACOSTA	\$673.00
12:31:01	CAROLYN M. ADAMS	\$1,120.00
12:34:12	MARY R. AKINS	\$1,815.00
12:39:06	MATTHEW S. ALVAREZ	\$1,668.00
12:45:42	MARTIN M. AGUAYO	\$418.00
12:51:29	BRIAN W. ALBOHER	\$1,452.00

Verizon Wireless broadband access card connection records for the Travis Rupard account (obtained pursuant to an Order issued pursuant to 18 U.S.C. 2703(d)) showed multiple connections to IP address 74.73.116.37 on May 25, 2008, as early as 7:10:14 p.m. GMT and as late as 7:59:36 p.m. GMT. Therefore, it appeared that the Aircard was used to file each of these fraudulent returns.

The AFDC reported the following fraudulent returns were filed on May 26, 2008, using IP address 67.187.132.91, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
20:05:49	LOREN L. AISENBREY	\$1,572.00
20:07:03	WALTER F. ALEXANDER	\$1,747.00

20:08:05	DAVID ALVAREZ	\$575.00
20:09:18	SHARON M. ADAMS	\$1,447.00
20:15:03	BART AGUIRRE	\$425.00
20:23:03	PATRICK ALDERETE	\$652.00
20:24:20	GLORIA A. AGANZA	\$1,939.00
20:27:57	EUGENE A. ALCANTER	\$1,246.00
20:29:15	MANUEL M. ADVIENTO	\$1,457.00

Verizon Wireless broadband access card connection records for the Travis Rupard account (obtained pursuant to an Order issued pursuant to 18 U.S.C. 2703(d)) showed multiple connections to IP address 67.187.132.91 on May 27, 2008, as early as 2:54:47 a.m. GMT and as late as 3:58:26 a.m. GMT. Therefore, it appeared that the Aircard was used to file each of these fraudulent returns.

The AFDC reported the following fraudulent returns were filed on May 27, 2008, using IP address 67.64.43.108, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
11:21:03	MICHAEL ALDERSON	\$1,436.00
11:23:20	ROBERT M. AASE	\$1,470.00
11:27:31	AHMAD R. ALFRED	\$924.00
11:35:15	ROBERT J. ADAME	\$2,130.00
11:39:59	JAMES E. ADAMS	\$1,763.00
11:42:03	DELAWARENCE L. ADKINS	\$1,981.00
11:47:23	LEONARD S. ABEYTA	\$1,420.00
11:48:58	LIZABETH A. AGUILAR	\$655.00
11:50:52	WAYNE A. ABEL	\$725.00
11:56:09	DANIEL E. ALBRIGHT	\$1,200.00
11:59:40	BRENT C. ALLRED	\$987.00

Verizon Wireless broadband access card connection records for the Travis Rupard account (obtained pursuant to an Order issued pursuant to 18 U.S.C. 2703(d)) showed the Travis Rupard account connecting with multiple connections to IP address 67.64.43.108 on May 27, 2008, as

early as 6:18:31 p.m. GMT and as late as 7:04:01 p.m. GMT. Therefore, it appeared that the Aircard was used to file each of these fraudulent returns.

The AFDC reported the following fraudulent returns were filed on May 28, 2008, using IP address 66.42.152.107, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
13:14:46	MARCIA ADKINS	\$1,056.00
13:16:07	BETTY A. ABRIL	\$981.00
13:20:02	DARLENE ALARCON	\$1,302.00
13:21:27	SERGIO R. AGUILAR	\$1,103.00
13:22:54	GERALD D. AKERS	\$1,188.00
13:25:47	BRYAN M. ACOSTA	\$1,326.00
13:27:15	GARY L. ALDINGER	\$1,865.00
13:28:40	DANIEL E. ADAMS	\$2,045.00
13:30:04	MARIO N. AGUIRRE	\$593.00
13:40:18	MICHAEL G. ALLEN	\$1,238.00
14:09:54	MARK S. ADLER	\$1,166.00
14:11:48	JULIA L. AKMAN	\$1,413.00
14:14:40	RAYMOND ALVAREZ	\$2,081.00
14:17:18	CHARLES O. ALIANO	\$1,079.00

Verizon Wireless broadband access card connection records for the Travis Rupard account (obtained pursuant to an Order issued pursuant to 18 U.S.C. 2703(d)) showed the Travis Rupard account with multiple connections to IP address 66.42.152.107 on May 28, 2008, as early as 8:13:27 p.m. GMT and as late as 9:17:22 p.m. GMT. Therefore, it appeared that the Aircard was used to file each of these fraudulent returns.

The AFDC reported the following fraudulent returns were filed on June 1, 2008, using IP address 68.198.200.5, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
11:43:48	THOMAS G. ANDRADE	\$1,525.00

11:50:06	ARTHUR R. ALVAREZ	\$1,651.00
11:51:28	GLORIA J. ARMIJO	\$1,910.00
11:53:14	DALE W. AMBLER	\$2,592.00
11:55:27	DALE B. ALFORD	\$950.00
12:14:59	ROBERT G. AMMONS	\$2,854.00
12:38:03	DAVID A. ALFATHER	\$888.00
12:39:37	MICHELLE L. ANDREWS	\$2,562.00
12:41:08	ROBERTO A. ALVAREZ	\$1,935.00

Verizon Wireless broadband access card connection records for the Travis Rupard account (obtained pursuant to an Order issued pursuant to 18 U.S.C. 2703(d)) showed the Travis Rupard account with multiple connections to IP address 68.198.200.5 on June 1, 2008 as early as 6:42:21pm GMT and as late as 7:42:48pm GMT. Therefore, it appeared that the Aircard was used to file each of these fraudulent returns.

The AFDC reported the following fraudulent returns were filed on June 3, 2008, using IP address 67.64.43.108, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
13:16:53	DAVID C. ALBERTSON	\$2,443.00
13:27:16	JESUS E. ALVARADO	\$2,349.00

Verizon Wireless broadband access card connection records for the Travis Rupard account (obtained pursuant to an Order issued pursuant to 18 U.S.C. 2703(d)) showed the Travis Rupard account with multiple connections to IP address 67.64.43.108 on June 3, 2008, as early as 8:13:09 p.m. GMT and as late as 8:47:38 p.m. GMT. Therefore, it appeared that the Aircard was used to file each of these fraudulent returns.

The AFDC reported the following fraudulent returns were filed on June 3, 2008, using IP address 76.229.232.193, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
13:50:37	KIM W. ALLEN	\$2,736.00
13:52:39	MICHAEL A. AMATUCCI	\$2,211.00

13:55:17	JENNIFER L. BARNUM	\$2,774.00
14:04:01	PATRICIA E. ALLEN	\$2,842.00
14:06:49	JAMES D. ALTUM	\$2,741.00
14:23:29	MARIA D. BARRAZA	\$2,842.00
14:25:08	JOSE A. ALVARENGA	\$2,481.00
14:26:36	AMBER D. BARFIELD	\$2,964.00
14:28:25	KAREN D. ALEXANDER	\$2,335.00
14:39:03	JAMES B. ALEXANDER	\$2,113.00
14:40:36	SCOTT A. ANDERSON	\$2,722.00
14:45:11	TRISHA L. BARTLETT	\$2,353.00
14:49:01	LEO L. ALBERT	\$2,241.00

Verizon Wireless broadband access card connection records for the Travis Rupard account (obtained pursuant to an Order issued pursuant to 18 U.S.C. 2703(d)) showed the Travis Rupard account with multiple connections to IP address 76.229.232.193 on June 3, 2008, as early as 8:48:23 p.m. GMT and as late as 10:07:17 p.m. GMT on June 3, 2008. Therefore, it appeared that the Aircard was used to file each of these fraudulent returns.

The AFDC reported the following fraudulent returns were filed on June 4, 2008, using IP address 67.172.220.94, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
23:16:11	RICK I. ALLISON	\$984.00
23:32:26	DANIEL L. ALLEN	\$2,556.00
23:33:56	RAYMOND J. ALVAREZ	\$1,557.00
23:37:44	ROSARIO V. ALTURA	\$2,966.00
23:48:40	SALLY M. BANDA	\$1,549.00
23:52:18	JAMES L. ALSUP	\$2,260.00
23:57:18	MANUEL S. ALLEN	\$2,928.00

Verizon Wireless broadband access card connection records for the Travis Rupard account (obtained pursuant to an Order issued pursuant to 18 U.S.C. 2703(d)) showed the Travis Rupard account with multiple connections to IP address 67.172.220.94, on June 5, 2008 as early as



6:06:42 a.m. GMT and as late as 7:06:36 a.m. GMT. Therefore, it appeared that the Aircard was used to file each of these fraudulent returns.

The AFDC reported the following fraudulent returns were filed on June 5, 2008, using IP address 67.187.119.170, with refunds destined for the undercover Bank of America account:

IP Time (PDST)	Name	Refund Amount
00:13:58	MELVIN G ARNOLD	\$1,629.00
00:16:25	CHRISTINE A ARENA	\$934.00
00:18:11	ANDREW L ALLISON	\$2,886.00
00:28:37	RACHELLE M BARROWS	\$1,405.00
00:32:58	CORLAINE R ALTO	\$1,955.00

Verizon Wireless broadband access card connection records for the Travis Rupard account (obtained pursuant to an Order issued pursuant to 18 U.S.C. 2703(d)) showed the Travis Rupard account with multiple connections to IP address 67.187.119.170 on June 5, 2008, as early as 7:08:22 a.m. GMT and as late as 7:40:29 a.m. GMT. Therefore, it appeared that the Aircard was used to file each of these fraudulent returns.

### 13. Analysis of Bank Accounts

The AFDC had identified refunds destined for the undercover bank accounts and continued to monitor the accounts for additional fraudulent returns. In addition, the AFDC used the information from the electronically filed returns to identify any additional fraudulent tax returns, IP addresses and/or accounts being used to facilitate the scheme. As of June 26, 2008, the following banks had been identified as being linked to this bulk filing scheme:

Bank	No. of Accounts	No. of Returns
Meridian Bank (Undercover Account)	1	395
Columbus Bank & Trust	1	73
Centennial Bank	23	200
GE Money Bank	3	134
Bancorp Bank	9	53

MetaBank	30	156
Arkansas State Bank	3	10
Bank of America (Undercover Account)	1	249
International Bank	2	2

Centennial Bank was identified the Centennial Bank accounts noted in the chart immediately above as being related to a debit card program that was issued by Galileo Processing, an intermediary processor as discussed further below.

Bancorp Bank identified the Bancorp accounts noted in the chart immediately above as being related to prepaid debit cards where the funds are loaded to the card at authorized third party locations, or electronically by direct deposit. A representative of the bank advised an IRS-CI special agent that the tax refunds deposited into the account were listed in the names of people other than the account holder.

A representative of MetaBank had informed an IRS-CI special agent that the MetaBank accounts noted in the chart immediately above were related to debit cards. The representative further explained that cards with account numbers starting with a 5 were from Account Now, the account numbers starting with a 7 were from NetSpend, and the accounts beginning with 065 were from Galileo Processing Inc.

According to Account Now Inc's website, [www.accountnow.net](http://www.accountnow.net), they were a premier provider of financial solutions for the millions of consumers in the United States who did not have established credit or traditional banking relationships. Account Now offered prepaid Master Cards. Account Now stated their prepaid Master Cards were issued by MetaBank. Deposits could be made to the account by paycheck, direct deposit or MoneyGram Express Payment.

According to NetSpend Corporation's website, [www.netspend.com](http://www.netspend.com), this company offered all access prepaid Visa and Master Card debit cards. The company's website stated that the cards worked like debit cards, without the hassle of a bank account and were accepted at millions of places worldwide. The website stated that a person could obtain a card without a credit check.

1 Funds were loaded on the card via direct deposit, by visiting a reload center or online with  
2 PayPal. Cards could be purchased at certain reload centers or through the website. NetSpend  
3 stated on their website that they were an authorized Independent Sales Organization of Inter  
4 National Bank and MetaBank and the cards were issued through these two banks.

5 According to Galileo Processing, Inc.'s website, [www.galileoprocessing.com](http://www.galileoprocessing.com), the  
6 company offered partners, clients, and consumers solutions and support for financial payment  
7 processing. According to the company's website, Galileo Processing, Inc., was an advanced  
8 processor for credit, debit, and prepaid card programs. The company offered multi purse  
9 technology, a proprietary bill payment service, integrated ACD and IVR, world class customer  
10 service, and real time connectivity to over 100,000 retail locations that accepted cash loads to  
11 prepaid cards.

12 14. The California Death Index

13 The social security numbers listed on the 395 tax returns identified with refunds destined  
14 for the IRS controlled undercover bank account at Meridian Bank and the 249 tax returns  
15 identified with refunds destined for the IRS controlled undercover account at Bank of America  
16 were researched on the California Death Index. The California Death Index contains millions  
17 of records with information for birth years 1940 through 1997. All 654 corresponding social  
18 security numbers were located using this data base. Research revealed that all of the individuals  
19 listed on these returns were deceased well before 2007, and therefore, did not receive taxable  
20 income in the form of wages in 2007.

21 15. E-Mail Communications Between the "Hacker" and CI 2

22 In the course of the execution of a Search Warrant on April 15, 2008, of a computer used  
23 by CI 2, e-mail records were recovered which had been sent on or before April 15, 2008, by the  
24 Hacker.

25 In an e-mail sent on unknown date prior to April 15, 2008, the Hacker advised CI 2 that  
26 he produces fraudulent identification documents and that he has sold identification documents  
27 for many years without any problems. The Hacker stated if he is raided by law enforcement, he  
28

1 will use his keystroke kill switch to shut down the computer and then physically hold down the  
2 power button to turn off the computer in case the kill switch fails. When the computer is shut  
3 down, all saved encryption keys will be deleted from the computer memory. Moreover, the  
4 "Hacker's" entire hard drive is always encrypted. (Fortunately for the investigation team, prior  
5 to the execution of SW 08-70460, the defendant was arrested nearby while outside of his  
6 apartment. When entry was made pursuant to the search warrant, defendant's computer was  
7 found to be unsecured and logged on, no password was needed in this instance in order to access  
8 the files.)

9 In an e-mail sent on unknown date prior to April 15, 2008, the Hacker also advised CI 2  
10 he uses a different IP address for each tax return and has filed returns with many different efilers.  
11 The Hacker believed filing the returns in this manner would prevent "them," (i.e., the IRS), to  
12 link them all. The Hacker advised an e-filer "took some heat" from the IRS because of his  
13 automated filing scheme. The Hacker stated the e-filer tried to stop him by use of a captcha, i.e.  
14 a box that appears on a webpage requiring the user to personally view a screen and then enter  
15 in a series of characters. The purpose of a captcha is to prevent automated entry of data on a  
16 webpage.

17 In an e-mail sent on unknown date prior to April 15, 2008, the Hacker advised CI 2 he  
18 knew "everything there is to know about creating new identities in the USA and I know a lot  
19 about assumed identities." The Hacker advised CI 2 he is an encryption expert and a privacy  
20 expert. Further, during a debriefing of CI 2 after April 15, 2008, he/she advised that the Hacker  
21 had obtained proceeds from the subject bulk filing scheme in the past through the receipt of  
22 encrypted electronic information regarding debit cards. CI 2 also stated that he/she has sent  
23 related account information to the Hacker which he could then use to create his own debit cards  
24 using an electronic debit card reader/writer and then withdraw the funds from automatic teller  
25 machines. In the course of follow-up investigation with respect to this information, an unknown  
26 white male or males, average build, appearing to between the age of 20 and 29, had been  
27 observed making withdrawals, or attempting to make withdrawals, with multiple debit cards  
28

1 from automatic teller machines on security camera photos obtained via Grand Jury subpoenas.  
2 In each case in March and April of 2008, the subject debit card accounts had previously received  
3 fraudulent tax refunds that had been obtained as part of the scheme.

4 On or about April 23, 2008, the Hacker advised CI 2 in an e-mail he had burned his  
5 identification document and his birth certificate. The Hacker stated to CI 2, "I am probably the  
6 single biggest threat to the US government currently living and they don't even know it. I can  
7 do things to the government that will make all these terrorist organizations look like sewing  
8 circles." In this same e-mail, the Hacker claimed to have a contact with an individual who was  
9 previously a United States Intelligence Agent who assisted the Hacker primarily with  
10 information on identities. The Hacker claimed he traded computer information with this former  
11 Intelligence Agent in exchange for information known to the former Intelligence Agent. The  
12 Hacker claimed this individual feared being accused of treason even though the former  
13 Intelligence Agent had not worked in the government for ten years.

14 On or about May 12, 2008, the Hacker e-mailed CI 2 and stated "I was thinking of  
15 starting with robotic aerial assassins that can be controlled from a computer over the internet.  
16 It would be essentially a flying handgun that no one would likely see. Perfect for taking out  
17 politicians. The controls would be military grade but designed by me. I was also thinking about  
18 making 50 mile range missiles without the warheads . . . I would only want to arm militias  
19 planning on standing up against the feds when the winner take all war takes place in the US . .  
20 . I am also trying to convince some old friends to help out with chemical and biological weapons  
21 as well. There will be no rules in this war. The government has already set the stage . . ." The  
22 Hacker added, "I have always wanted a small automatic weapon with a silencer similar to the  
23 one Bruce Willis used in Pulp Fiction to kill the Scientologist . . ." The Hacker advised CI 2,  
24 "If you can help me expand my arsenal then I would appreciate it" (The weapon used in the  
25 movie appears to be a handheld machine gun with a silencer.)

26 On or about May 14, 2008, the Hacker e-mailed CI 2 a list of numerous weapons to  
27 follow up on. In numerous subsequent e-mails, the Hacker engaged in discussions regarding  
28

1 purchasing an unregistered MAC-10 with a silencer with CI 2 serving as a broker. On or about  
2 June 2, 2008, the Hacker e-mailed CI 2 that, "I have a lot of money to spend on guns (100k+)  
3 but if this is what it is like to deal with illegal gun dealers then I will stick to making AR15s,  
4 AK47s and M4s in my garage." The Hacker decided not to purchase the weapon at that time but  
5 advised he would consider purchasing a weapon in the future through CI 2.

6 On or about May 23, 2008, the Hacker sent an e-mail to CI 2 asking for access to the  
7 Social Security Administration internal "death master file". The Hacker believed this death  
8 index contained information on deaths of persons for whom the Social Security Administration  
9 has not been able to verify the deaths and therefore cannot treat these persons as deceased for  
10 tax purposes. The Hacker asked CI 2 for other personal identifying information in database  
11 format and access to information in a state death database for persons who died in the year 2008.  
12 It was believed that the Hacker sought and continued to seek personal identifying information  
13 on individuals that he could utilize to file fraudulent tax returns. Since CI 2 successfully  
14 provided the Hacker with \$68,000.00 in cash, the "Hacker's" opinion of CI 2's capabilities as  
15 a middleman were greatly enhanced.

16 On or about June 10, 2008, the Hacker sent an e-mail to CI 2 stating, "I funded other bank  
17 accounts at the same time from the same proxies and they all work out . . . " It was believed that  
18 the Hacker was referencing fraudulent tax returns sent to other accounts in addition to the Bank  
19 of America undercover bank account.

20 On or about June 11, 2008, the Hacker sent an e-mail to CI 2 asking for personal  
21 identifying information of third parties. The Hacker again sought information on the Social  
22 Security Administration "internal death master file," the previous Choicepoint data compromise,  
23 and personal identifying information on Bank of America customers. The Hacker further  
24 advised that, "I can and will bring this country into a "Mad Max" state if the government  
25 continues down their path. I just hope there are enough people with enough guns spread through  
26 out the country to fight off the feds and split the country into new countries . . . " It was believed  
27 that the reference to Mad Max refers to the post-apocalyptic world depicted in the film "Mad  
28

1 Max.” (During the execution of defendant’s apartment pursuant to SW 08-70460 and a  
2 subsequent search of a storage locker rented by defendant under the additional false identity  
3 “Daniel Clifton Aldrich,” pursuant to the execution of Northern District of California Search  
4 Warrant No. 08-70502-PVT, authorized on August 4, 2008, no firearms were found.)

5 On or about June 26, 2008, the Hacker warned CI 2 about the countermeasures he would  
6 use to take possession of a bulk currency delivery he was owed after June 30, 2008, which  
7 represented his percentage of the proceeds derived from fraudulent tax returns. The Hacker  
8 advised that the courier who would retrieve the package containing the bulk currency from the  
9 mailing center would be armed with a concealed M4 assault rifle. The Hacker stated the courier  
10 would scan the package for both analog and digital radio signals and with an ultraviolet black  
11 light. The Hacker advised CI 2 that if the package was transmitting a radio frequency signal or  
12 the tape on the package had been replaced, the courier would run away and shoot anyone who  
13 tried to grab him. According to the Hacker, a team would be in place to provide cover fire so  
14 all members of the pickup team could escape. The Hacker advised if anything happened in the  
15 FedEx center, “everyone who works there will be dead.” The Hacker advised if anything  
16 happened outside the FedEx store, then anyone the pickup team saw would be dead and any cops  
17 would be dead. The Hacker stated the pickup team would “make a point” by killing innocent  
18 people just to teach law enforcement a lesson. On the chance that CI 2 was a CI, the Hacker  
19 planed on e-mailing unidentified reporters, in encrypted fashion, the exact details of the package  
20 pickup and the countermeasures in place to prove that CI 2 knew beforehand that people would  
21 die if law enforcement intervened. If a law enforcement sting ensued at the FedEx store, the  
22 Hacker would then e-mail the passwords to the encrypted messages previously sent to the  
23 reporters so that the news would be, “Law Enforcement and CI knew about murderous rampage  
24 but did nothing to prevent it!”

25 16. Historical Cell Tower Information and Other Investigative Techniques

26 Historical cell tower information for the Aircard and the records relating to the use of  
27 particular IP Addresses used by the card as described above, lead to the conclusion that the  
28



Hacker had used the Aircard to commit offenses in violation of numerous federal statutes set forth in the affidavit as follows:

- a. 18 U.S.C. § 286 - Conspiracy to Defraud the Government;
- b. 18 U.S.C. § 287 - False, Fictitious or Fraudulent Claims;
- c. 18 U.S.C. § 371 - Conspiracy;
- d. 18 U.S.C. § 1028 - Fraud Related to Identity Information;
- e. 18 U.S.C. § 1028A - Aggravated Identity Theft;
- f. 18 U.S.C. § 1029 - Fraud with Access Devices;
- g. 18 U.S.C. § 1341 - Mail Fraud;
- h. 18 U.S.C. § 1343 - Wire Fraud;
- I. 18 U.S.C. § 1030 - Computer Abuse and Fraud

The affidavit further advised that historical cell tower information and other investigative techniques had led the investigation team to the location of the Aircard within the “Domicilio” apartment complex; 431 El Camino Real; Apartment 1122; Santa Clara, California, 95050.

On July 17, 2008, a Grand Jury subpoena was issued to Domicilio for the file information related to 431 El Camino Real, Apartment 1122, Santa Clara, California, 95050. The subpoena revealed the apartment was currently being rented by an individual claiming to be Steven Travis Brawner. The rental application indicated Brawner was a software engineer.

Brawner provided a California driver’s license, license number D6870214. Further investigation revealed the California driver’s license number was assigned to a female with a Chino Hills, California address.

In order to rent the apartment, Brawner was required by the rental company to provide a copy of the first page of what he claimed to be this 2006 tax return. The return purported to show an adjusted gross income of \$110,314. The social security number on the return was 559-87-4167. Internal records for the Internal Revenue Service were researched and revealed no tax return for 2006 was filed for Steven Travis Brawner. Additionally, Social Security Administration records for social security number 559-87-4167 indicated that Steven Brawner died in 1997.

On July 21, 2008, Forensic Document Examiner William J. Flynn conducted a handwriting analysis of the original application documents for 431 El Camino Real, Apartment 1122 and the original application documents for the (Patrick Stout) Sacramento Post Office Box.

1 After conducting the analysis of the documents, Mr. Flynn advised that forensic evidence  
2 indicated common authorship among the documents.

3 The Domicilio apartment complex located at 431 El Camino Real, Santa Clara, California  
4 95050 was a gated community, with a unique "fob number" assigned per individual for key card  
5 access. In response to a Federal Grand Jury subpoena issued to the Domicilio apartment  
6 complex, it was determined that fob number 58261 was assigned to the individual purporting to  
7 be Steven Travis Brawner. The investigation revealed the gate access system service was  
8 provided by Quality Alarm. In response to a Federal Grand Jury subpoena issued to Quality  
9 Alarm regarding fob number 58261, records showed that the individual purporting to be Steven  
10 Travis Brawner accessed the Domicilio apartment complex sixteen separate times between June  
11 4, 2008 and July 23, 2008. Of the sixteen separate accesses, nine of the accesses were made  
12 between the hours of 10:00 pm until 6:00 am.

13 During the month of July 2008, daytime surveillance and spot check surveillance were  
14 unable to observe any residents at the subject location. On July 22, 2008, at approximately 7:20  
15 pm, an FBI Special Agent acting in an undercover capacity knocked on the door using the ruse  
16 of a fast food delivery. No one answered the door.

17 This information set forth above is a summary of the information set forth in the affidavit  
18 submitted in support of the application for SW 08-70460.

19 Shortly after the investigation team had narrowed down the focus of their investigation  
20 to a particular apartment within the apartment complex, the rental agency allowed the team to  
21 use a nearby vacant apartment in order to conduct surveillance. From July 16, 2008, through the  
22 afternoon of August 3, 2008, no one matching "Steven Brawner's" description was seen coming  
23 into, or out of, the apartment occupied by defendant. The rental agency continued to grant the  
24 investigation team access to the apartment complex until well after the defendant's arrest and the  
25 execution of SW 08-70460 in the late afternoon of August 3, 2008.

1           17.     The “Aircard Mission”

2           The tracking device warrant, CR 08-90330MISC (CR 470-1), was issued July 11, 2008,  
3 and was based on a finding of probable cause to believe that the use and monitoring of a tracking  
4 device would lead to evidence of crime and the identification of the perpetrator. The warrant also  
5 compelled Verizon Wireless to assist as necessary. The warrant specifically allowed monitoring  
6 of the aircard for up to 30 days, day or night, even if the aircard was located inside a private  
7 residence.

8           In order to locate the subject Aircard, FBI Special Agent Kevin Killigrew first used  
9 historical cell tower information obtained pursuant to Orders issued pursuant to Section 2703(d)  
10 related to the subject Aircard’s account with Verizon Wireless, and information provided to him  
11 to the FBI from Verizon Wireless regarding the operation and range of the firm’s cell towers and  
12 related equipment, and his personal training and experience in order to estimate the general  
13 location of where the Aircard may have been used in the passed based upon which cell towers  
14 the Aircard had communicated with and the estimated range of the subject cell towers. Based  
15 upon this information, the investigation team was directed to commence further efforts to locate  
16 the Aircard within an area within Santa Clara, California. In preparation for the next step in the  
17 Aircard Mission, the investigation team obtained the following orders in the Northern District  
18 of California, Order No. CR-08-90330, In the Matter of the Application of the United States of  
19 America for an Order Authorizing the Use and Monitoring of a Mobile Tracking Device and  
20 Order No. CR-08-90331 (CR 470-2), In Re Telephone Information Needed for a Criminal  
21 Investigation.

22           For the purpose or addressing defendant’s motion to suppress, the United State made the  
23 following concessions in Government’s Memorandum Re Motion For Discovery (CR 674,  
24 footnotes omitted). First, the United States proposed that the Court assume, arguendo, for  
25 defendant’s Motion for Discovery and any forthcoming Motion to Suppress, that the aircard  
26 tracking operation was a Fourth Amendment search or seizure.

1 Second, the United States agreed to rely solely on the Rule 41 tracking warrant,  
2 application and affidavit, No. CR-08-90330-MISC, to authorize the use of the equipment to  
3 communicate directly with the Aircard and determine its location.

4 Third, the United States agreed to allow the Court to factually assume, that, at the  
5 conclusion of the July 16, 2008, aircard tracking operation, the FBI located the aircard within  
6 Unit 1122 of the Domocilio Apartments.

7 Fourth, with respect to whether the equipment used to locate the Aircard was operated  
8 in a “man-in-the-middle” manner or caused a “disruption of service,” the United States agreed  
9 to that the Court can assume, arguendo, that it did. In the affidavit attached to the Memorandum,  
10 FBI Special Agent Bradley Morrison noted that the equipment in this case did not capture any  
11 content and it did not act as a “man in the middle” collecting data and passing it on to Verizon  
12 Wireless. (CR 674-1, ¶ 4).<sup>2/</sup>

13 18. The Arrest of the Hacker

14 On August 3, 2012, at approximately 4:15 p.m., two federal agents were conducting their  
15 ongoing surveillance of the exterior of the subject apartment. An unidentified person matching  
16 the description of the resident of the subject apartment, “Steven Brawner,” was observed  
17 walking away from an area near the apartment. The agents started to follow the person in order  
18 to attempt to further identify him. At this time, the original indictment in this case was sealed  
19 and there was a companion outstanding arrest warrant for Steven Travis Brawner, a.k.a. Travis  
20 Rupard, a.k.a. Patrick Stout. While the unidentified person was being followed, he began to act  
21 in a manner that was suspicious to the agents. Fortuitously, one of the federal agents was able  
22 to flag down a local Santa Clara Police Department marked unit occupied by two uniformed  
23 officers. The local officers agreed to assist the federal agents in the apprehension of a federal  
24

---

25 <sup>2/</sup> Defendant notes that the last record of contact with the Aircard was at approximately  
26 5:03 p.m., July 16, 2008. Mot. at 179-80. Defendant inadvertently concluded that the location  
27 mission continued until approximately 2:42 a.m., July 17, 2008, based upon a FBI text that was  
28 sent noting that the apartment had been located. Mot. at 180. The subject text records were  
prepared using Greenwich Mean Time, therefore the actual approximate date and time of the text  
(7 hours earlier) was 7:42 p.m., July 16, 2008.

1 fugitive. At least one other local police department marked unit was then also on its way to  
2 assist. The initial four law enforcement officers then attempted to locate the subject. One of the  
3 federal agents observed the subject as he appeared to be hiding near a coffee shop. The subject  
4 then appeared to be running through a parking lot and then eventually ran into a nearby street  
5 against traffic. The second marked unit approached the subject head on and he ran into the  
6 opposite lanes and was now running in the direction of the traffic. One of the marked units  
7 attempted to block the subject, he ran into the unit and was apprehended. The subject resisted  
8 arrest by rocking left to right and kicking with his feet. Once secured, the subject did not appear  
9 to have suffered any serious injuries. At this point, the subject refused to identify himself. A  
10 search of his person located a small amount of money and a set of keys. No form of  
11 identification was found on the subject. The subject appeared to match the image of the person  
12 in the driver's license photo that had been provided with the subject apartment's rental  
13 application. A third federal agent was summoned to the scene from the nearby apartment  
14 complex. The third agent took the keys which had been seized incident to arrest and went back  
15 to the subject apartment.

16 A this time, the investigation team had in its possession sealed SW 08-70460 for the  
17 subject apartment. Within a short time after the arrest, the third agent took the subject keys to  
18 the subject apartment and tested them in the apartment's front door lock. One of the keys turned  
19 the lock. The agent did not open the door or enter the apartment. The agent called one of the  
20 arresting federal agents who was still at the scene with the subject and advised that one of the  
21 keys fit the lock. The subject was transported for processing at that time. The third agent  
22 remained outside of the subject apartment and helped to maintain the security of the apartment  
23 until additional federal agents arrived and entry was made pursuant to the warrant at 5:20 p.m.

24 The subject was ultimately identified via fingerprint analysis as the defendant Daniel  
25 David Rigmaiden, a fugitive with a 2000 outstanding arrest warrant in an unrelated fraud case  
26 in Santa Cruz County, California. A plethora of evidence found in the apartment and in the  
27  
28

1 defendant's computer tied the defendant to his apartment, including numerous pieces of false  
2 identification bearing his defendant's photographic image.

3       Until defendant's arrest pursuant to an arrest warrant, the investigation team took no steps  
4 to interfere with his liberty interests due to the fact they had never fully identified or contacted  
5 prior to his arrest, and the only steps that could have possibly been taken to interfere with his  
6 possession of any item, in this case the Aircard (setting aside for the moment whether defendant  
7 had any reasonable expectation of privacy in the Aircard), were the efforts conducted by the FBI  
8 in the course of locating the Aircard on July 16, 2008; steps which were so insignificant they  
9 went undetected by defendant.

10       19.     The Defendant's Numerous False Identities Used to Procure and Maintain the  
11               Aircard and Its Aircard Account, the Apartment and the Laptop and Electricity  
              Used to Operate the Aircard

12       By means of introduction, the investigation team has yet to uncover a single means by  
13 which the defendant had lawfully earned any money for many years prior to arrest. Therefore,  
14 while defendant claims to have paid for things with "his money," there is no known lawful  
15 source for any of the money he used to purchase or maintain the Aircard, lease or maintain the  
16 apartment he used as the base of his criminal operations, and purchase the laptop and electricity  
17 he used to run the Aircard, all of which he used to commit the offenses listed above and in the  
18 superseding indictment.

19       A.     Travis Rupard, the Aircard and the Aircard Account

20       The Aircard was purchased from Verizon Wireless by defendant using the false identity  
21 of another living person, Travis Rupard, on or about May 23, 2006. IRS-CI has determined that  
22 at the time of the Aircard's purchase, the true Travis Rupard was alive and the resident of a State  
23 other than California. Defendant maintained an account with Verizon Wireless for cellular  
24 service for the Aircard under the same false identity at least until the day of his arrest. In order  
25 to back- stop the false identity of Travis Rupard, defendant provided the actual Social Security  
26 Number for the true Travis Rupard and the address for a PO Box in San Jose, California, to  
27 Verizon Wireless. The application for the San Jose PO Box was also made under the false  
28

1 identity of Travis Rupard, and back-stopped with a false driver's license and false identification  
2 card for a university. The PO Box was opened on March 13, 2006 and closed on August 31,  
3 2006.

4 B. Steven Brawner and the Apartment

5 Defendant applied for a lease for his apartment on October 18, 2007, using the false  
6 identity of Steven Brawner. In order to obtain the lease, defendant provided a forged California  
7 driver's license and the first page of a forged Federal income tax return which bore the true  
8 social security number for Steven Brawner who was deceased. The Brawner rental application,  
9 forged page of a tax return and driver's license were all back-stopped by a different PO Box in  
10 San Francisco, California. The San Francisco PO Box was applied for on September 27, 2006  
11 and back stopped by a different fraudulent driver's license and fraudulent student identification.  
12 At the time of his arrest, defendant was living in the apartment under the false Brawner identity  
13 with no means of traceability or recourse if he walked away from the terms of the lease or  
14 apartment.

15 C. Andrew Johnson and the Laptop Used to Operate the Aircard

16 On September 13, 2007, defendant purchased the laptop used to operate the laptop from  
17 Lenovo with the false identity of Andrew Johnson, a deceased individual. The purchase was  
18 made with a Galileo Processing Visa card with the false identity of Andrew Johnson. The  
19 application for the Visa card was back-stopped by the true Social Security Number for Andrew  
20 Johnson and a different PO Box in San Francisco opened under the false identity of Andrew  
21 Johnson.

22 20. The Search of the Seized Computers

23 As stated above, the investigation team executed SW 08-70460-HRL for defendant's  
24 apartment on August 3, 2008. Attachment C of the warrant consisted of a "Computer Search  
25 Protocol For The Northern District Of California," which detailed the procedures that the United  
26 States would follow for computer evidence. The protocol required, among other things, that the  
27 United States file a return within 10 days identifying the devices seized from the apartment. See  
28



1 SW 08-70460HRL at 2 ¶ 4. The protocol also required the United States to complete an off-site  
2 search of the seized devices within 30 days, and within the following 60 days the United States  
3 must return any devices that do not contain contraband or evidence of crime. See id. at 2 ¶ 5.  
4 Finally, the protocol states that the United States “must use reasonable efforts” to delete non-  
5 responsive material within the next 60 days (i.e., within 120 days of executing the warrant):

6       Within a reasonable period, not to exceed sixty calendar days after completing the  
7       authorized search of a device, the government also must use reasonable efforts to  
8       destroy—and to delete from any devices or storage media or copies that it has  
9       retained or made—copies of any data that are outside the scope of the warrant but  
10      that were copied or accessed during the search process, unless, under the law, the  
    government may retain the copies (1) to preserve evidence, or (2) because the  
    copies are contraband, a forfeitable instrumentality of the crime, or fruit of crime.  
    The deadlines set forth in this paragraph may be extended by court order for good  
    cause shown.

11 id.

12       The United States complied with the computer search protocol. The United States filed  
13 the return for the warrant on August 5, 2008, which is well within the 10-day time limit stated  
14 in the protocol. Moreover, the return included a detailed inventory of the devices and other items  
15 seized from the premises. The United States anticipates that IRS Special Agent Tracy Daun will  
16 testify that she personally conducted an initial review of the devices at the premises on the day  
17 the search warrant was executed, and on that day she found a file labeled filesalot.dcv that  
18 contained the bulk of the incriminating evidence. She will also testify that, within 30 days of the  
19 execution of the warrant, she created forensic copies, or “images,” of the seized devices and  
20 determined which of those devices contained material responsive to the search warrant. The  
21 images of devices or storage media that did not contain responsive material were destroyed by  
22 approximately August 28, 2008, which is less than 30 days after the execution of the warrant.  
23 This, too, satisfies the protocol, which required the United States to return the devices within 60  
24 days and delete images that do not contain responsive material within 120 days.

25       The United States retained forensic images of the devices that Agent Daun determined  
26 did contain evidence of crime, so that it could preserve the evidence and lay a proper foundation  
27 at trial. The United States also retained any devices that it determined contained contraband –  
28

e.g., stolen financial or identity information. With respect to the return of all of the devices or storage media that were not subject to seizure, the United States originally offered to return the items to defendant's prior defense counsel. In light of the fact they lacked storage space and defendant was in custody, the United States agreed to retain the items until further instructions were received from the defendant. The items have been stored and secured since they were originally mirrored shortly after their seizure. The items have not been searched since they were originally mirrored and remain available to be returned upon request.

Due to the volume of data on the devices, Agent Daun continued to analyze the seized evidence throughout 2009 and further identified information contained within the seized items. Any further searches to be conducted by Agent Daun will be limited to the materials she identified via her 2009 analysis. She will likely continue to analyze those digital materials pursuant to the warrant up through trial in this matter, much like a law enforcement agent continuing to analyze a firearm or other type of lawfully seized physical evidence.

## **II. Law & Argument**

Defendant's challenges numerous portions of the investigation that led to his arrest, the search of his apartment, and the seizure of a wealth of incriminating evidence. Ultimately, however, he is presenting three questions for the Court to decide:

- 1) Was the United States' collection of historical records pursuant to subpoenas and court orders reasonable?
- 2) Were the FBI's efforts to locate the aircard pursuant to the tracking warrant reasonable?
- 3) Was the subsequent search of his apartment and computer pursuant to the search warrant reasonable?

As argued below, the answer to each of these questions is yes. Defendant's motion should therefore be denied.

1. The United States' Collection Of Historical Records Pursuant To Subpoenas And Court Orders Was Reasonable.

Defendant challenges two categories of business records related to the account that the United States obtained pursuant to subpoena or a court order issued pursuant to 18 U.S.C. § 2703(d) (a “2703(d) order”). (See, e.g., CR 824-1 (“Mot.”) at 215-224, 239-249, 259-261, 283-284.) First, the United States obtained 2703(d) orders to compel Verizon Wireless to disclose historical cell site information and destination IP addresses for the Aircard. Second, the United States used grand jury subpoenas to compel the Domicilio Apartment Complex to turn over a copy of defendant’s rental agreement file and Quality Alarm Service to disclose its records regarding defendant’s entries into or out of the Domicilio Apartment Complex. Defendant argues that the Fourth Amendment required the United States to obtain a warrant to compel disclosure of this information. This argument is mistaken: a customer has no reasonable expectation of privacy in a corporation’s business records, and there is no warrant requirement for compulsory process. Moreover, because the government obtained this information based on good faith reliance on statutory and judicial authorization, as well as existing precedent, suppression is not an available remedy.

A. The Historical Records Were Properly Obtained Pursuant To Statute Or Rule.

A 2703(d) order may be used to compel disclosure of historical cell-site records or IP address records because these records fall within the scope of 18 U.S.C. § 2703(c)(1). In particular, 18 U.S.C. § 2703(c)(1) requires “a provider of electronic communication service . . . to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)” pursuant to a 2703(d) order. IP address records and cell-site records fall within the scope of this provision. First, ISPs and cell phone companies are providers of electronic communication service because they provide their users with “the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15). Second, an IP address record or a cell-site record is “a record or other information pertaining to a subscriber or customer of such service (not including the contents of communications).” Therefore, disclosure of IP address records and cell-site records may be obtained pursuant to 18 U.S.C. §§ 2703(c)(1) and (d). See In re Application of the United States, 620 F.3d 304, 313 (3d

1 Cir. 2010) (holding that historical cell site location information is “obtainable under at § 2703(d)  
 2 order”); United States v. Graham, 846 F. Supp. 2d 384, 396 (D. Md. 2012) (“It is well  
 3 established that Section 2703(c)(1)(B) of the Stored Communications Act applies to historical  
 4 cell site location data.”); In re Applications of the United States, 509 F. Supp. 2d 76, 79-80 (D.  
 5 Mass. 2007) (holding that historical cell site information “clearly satisfies” the definitional  
 6 requirements of § 2703(c) and is therefore obtainable under § 2703(d)).

7 Grand jury subpoenas were properly used to obtain records from the apartment rental  
 8 company and alarm service because “[a] subpoena may order the witness to produce any books,  
 9 papers, documents, data, or other objects the subpoena designates.” Fed. R. Crim. P. 17(c)(1).

10 B. Defendant Has No Privacy Interest In Any Of The Historical Records Obtained  
 11 By The United States in this Case.

12 The historical cell-site records, IP address records, and rental property and alarm service  
 13 records obtained by the United States are all business records. Setting aside for the moment that  
 14 the Aircard, the Aircard account, and the apartment's services such as security and utilities, were  
 15 all procured through the use of fraudulent identities, a customer has no privacy interest in  
 16 business records that are not the customer's private papers. Addressing a Fourth Amendment  
 17 challenge to a third party subpoena for bank records, the Supreme Court held in United States  
 18 v. Miller, 425 U.S. 435 (1976), that the bank's records “are not respondent's ‘private papers’”  
 19 but are “the business records of the banks” in which a customer “can assert neither ownership  
 20 nor possession.” Miller, 425 U.S. at 440. The records “pertain to transactions to which the bank  
 21 was itself a party.” Id. at 441. As the United States Court of Appeals for the District of  
 22 Columbia stated, “it has been consistently held by the Supreme Court and the Courts of Appeals  
 23 that a person has no Fourth Amendment basis for challenging subpoenas directed at the business  
 24 records of a third party.” Reporters Committee for Freedom of Press v. AT&T, 593 F.2d 1030,  
 25 1044 (D.C. Cir. 1978) (citing cases). In a case involving a subpoena for an electricity company's  
 26 power records, the Ninth Circuit recently confirmed that “[a] customer ordinarily lacks a  
 27 reasonable expectation of privacy in an item, like a business record, in which he has no  
 28

1 possessory or ownership interest.” United States v. Golden Valley Elec. Ass’n, \_\_\_ F.3d \_\_\_,  
2 2012 WL 3185827 (9th Cir. Aug. 7, 2012) (internal quotation marks omitted).

3       The reasoning of Miller applies to the historical records obtained by the United States.  
4 They are not the customer’s private papers. Once a customer makes a call, communicates over  
5 the Internet, leases an apartment, or uses the services of an alarm company, he has no control  
6 over the business record made by the business of that transaction. Instead, the record created  
7 is a business record of the provider. The choice to create and store the record is made by the  
8 provider, and the provider controls the format, content, and duration of the records it chooses  
9 to create and retain. Indeed, because these records are not in the possession of a customer, a  
10 customer could not be expected to produce the records in response to a subpoena. Moreover,  
11 these records pertain to transactions to which the companies were a participant. The assignment  
12 of a particular cell tower to process a call is made by the cell phone company to facilitate the  
13 functioning of its network; the ISP uses the IP address to route Internet communications it  
14 transmits; the rental company maintains a rental file for each occupant; and an alarm service  
15 independently maintains records of the equipment it installs and maintains. Thus, under Miller,  
16 the business records obtained by the government are not protected by the Fourth Amendment.

17       The Supreme Court’s reasoning in Smith v. Maryland, 442 U.S. 735 (1979), leads to the  
18 same result. In Smith, the Court held both that telephone users had no subjective expectation  
19 of privacy in dialed telephone numbers and also that any such expectation is not one that society  
20 is prepared to recognize as reasonable. See Smith, 442 U.S. at 742-44. The Court’s reasoning  
21 applies equally to the business records in this case. First, the Court stated: “we doubt that people  
22 in general entertain any actual expectation of privacy in the numbers they dial. All telephone  
23 users realize that they must ‘convey’ phone numbers to the telephone company, since it is  
24 through telephone company switching equipment that their calls are completed.” Id. at 742.  
25 Second, Smith held that “even if petitioner did harbor some subjective expectation that the phone  
26 numbers he dialed would remain private, this expectation is not one that society is prepared to  
27 recognize as reasonable.” Id. at 743 (internal quotation omitted). It noted that “[t]his Court  
28

1 consistently has held that a person has no legitimate expectation of privacy in information he  
2 voluntarily turns over to third parties.” Id. at 743-44. The user “voluntarily conveyed numerical  
3 information to the telephone company” and thereby “assumed the risk that the company would  
4 reveal to police the numbers he dialed.” Id. at 744.

5       The Ninth Circuit has explicitly held that Smith applies to IP address information. See  
6 United States v. Forrester, 512 F.3d 500, 510 (9<sup>th</sup> Cir. 2008) (“Internet users have no expectation  
7 of privacy in the to/from addresses of their messages or the IP addresses of the websites they  
8 visit because they should know that this information is provided to and used by Internet service  
9 providers for the specific purpose of directing the routing of information”). Similarly, cell phone  
10 users understand that they must send a radio signal which is received by a cell phone company's  
11 antenna if the company is going to route their call to its intended recipient. Indeed, cell phone  
12 users routinely experience the frustration associated with dropped calls and recognize they are  
13 caused when their phone’s radio signal is having difficulty reaching a tower clearly. Cell phones  
14 also often display a cell tower icon, along with bars representing the strength of the signal  
15 between the phone and tower. Cell phone users also understand that the provider will know the  
16 location of its own cell tower, and that the provider will thus have some knowledge of the user’s  
17 location. Furthermore, providers’ terms of service and privacy policies make clear that the  
18 provider obtain this information. Security system users understand that they must present their  
19 identifying information to the security system in order for the system to verify that they are  
20 entitled to access the premises. Finally, defendant was clearly concerned that he could somehow  
21 be identified through the acquisition and maintenance of the Aircard account as evidenced by  
22 his assumption of the identity of another person prior to purchasing the Aircard and his  
23 herculean attempts to mask the Aircard’s true IP address while committing a never ending series  
24 of crimes and communicating with his associates via encrypted e-mails. For example, in the  
25 months prior to his arrest, defendant traveled to another city in Northern California and was  
26 captured on a Verizon Wireless store's surveillance camera personally placing funds on his  
27 account at an automated kiosk. This conduct allowed defendant to not have to transmit or mail  
28

1 any funds to Verizon Wireless, or personally interact face-to-face with any employees, while he  
2 maintained the fraudulently obtained account.

3 Defendant makes various attempts to distinguish Miller and Smith, but these attempts are  
4 unavailing. For example, he argues that he “had no idea that Verizon Wireless collected  
5 historical cell site location information on his aircard use.” (Mot. 221.) The Supreme Court  
6 rejected this argument in Smith, where it held that “[t]he fortuity of whether or not the phone  
7 company in fact elects to make a quasi-permanent record of a particular number dialed does not  
8 in our view, make any constitutional difference.” Smith, 442 U.S. at 745. The Court explained  
9 that “[r]egardless of the phone company's election, petitioner voluntarily conveyed to it  
10 information that it had facilities for recording and that it was free to record.” Id. See also  
11 United States v. Skinner, \_\_\_ F.3d \_\_\_, 2012 WL 3289801 at \*4 (6th Cir. Aug. 14, 2012)  
12 (holding that locating defendant through a phone's cell site records is not a 4th Amendment  
13 search: “If a tool used to transport contraband gives off a signal that can be tracked for location,  
14 certainly the police can track the signal. The law cannot be that a criminal is entitled to rely on  
15 the expected untrackability of his tools.”); United States v. Gallo, 123 F.2d 229, 231 (2d Cir.  
16 1941) (L. Hand, Swan, A. Hand, JJ.) (“When a person takes up a telephone he knows that the  
17 company will make, or may make, some kind of a record of the event, and he must be deemed  
18 to consent to whatever record the business conveniences of the company requires.”).

19 Defendant attempts to distinguish Miller by arguing that the historical cell site records  
20 cannot be business records because they were produced to the United States in an Excel  
21 spreadsheet, which is not how Verizon Wireless stores the data. (Mot. at 219.) There is no  
22 requirement that the information produced pursuant to subpoena or court order be in the same  
23 format that the business itself uses to store the records. See, e.g., Fed. R. Civ. Proc. 45(a)(1)(C)  
24 (“A subpoena may specify the form or forms in which electronically stored information is to be  
25 produced.”), (d)(1)(B) (“If a subpoena does not specify a form for producing electronically  
26 stored information, the person responding must produce it in a form or forms in which it is  
27 ordinarily maintained or in a reasonably usable form or forms.”)



1 Defendant also argues that the records are invasive, suggesting that the third parties  
2 should not have created or maintained the records in the first place. (Mot. at 215-17 (discussing  
3 cell site information).) As an initial matter, the business records obtained by the United States  
4 are not particularly invasive. For example, historical cell site records reveal only past  
5 information about the general location of the aircard, and IP address records do not reveal the  
6 contents of communications. But in any case, the Supreme Court has never limited the principle  
7 of Miller and Smith v. Maryland — that information revealed to a third party may subsequently  
8 be conveyed to the government — to information that is unrevealing or of limited use to law  
9 enforcement. Indeed, United States v. Miller cites three cases for the proposition that "the  
10 Fourth Amendment does not prohibit the obtaining of information revealed to a third party and  
11 conveyed by him to Government authorities," and all three of these cases involve the content of  
12 communications, rather than the kind of non-content business records that are at issue here. See  
13 Miller, 425 U.S. at 443 (citing United States v. White, 401 U.S. 745 (1971) (content of  
14 conversation with informant), Hoffa v. United States, 385 U.S. 293 (1966) (content of  
15 conversations with or in presence of informant), and Lopez v. United States, 373 U.S. 427  
16 (1963) (content of conversation with government agent)). Obtaining the business records in this  
17 case was substantially less intrusive than obtaining the contents of communications.

18 United States v. Jacobsen further illustrates that the extent to which the third party  
19 business records are invasive however, that is not an appropriate basis for a Fourth Amendment  
20 challenge. 466 U.S. 109 (1984). In Jacobsen, a private freight carrier inspected a damaged  
21 package and found tubes full of white powder. Id. at 111. They turned the material over to law  
22 enforcement, who also inspected the package. Id. at 112. Jacobsen argued that opening the  
23 package and inspecting its contents violated the Fourth Amendment, but the Court explained that  
24 the search could not be a Fourth Amendment violation, even if it was unreasonable or invasive,  
25 because it was done by a private party:

26 The initial invasions of respondents' package were occasioned by private action.  
27 . . . Whether those invasions were accidental or deliberate, and whether they were  
28 reasonable or unreasonable, they did not violate the Fourth Amendment because  
of their private character.

1 Id at 115. Here, too, the cell site information that defendant worries will “allow[] the  
 2 government to infer that the defendant was a consistent homebody who rarely leaves his  
 3 apartment,” (Mot. at 217), was collected and maintained by a private party. It does not become  
 4 a Fourth Amendment search or seizure simply because the information is turned over to law  
 5 enforcement.

6 Defendant cites no case, and the United States is aware of none, in which a federal court  
 7 has ever suppressed cell-site records, IP address records, or security system records. As  
 8 previously noted, the Ninth Circuit has rejected a motion to suppress IP address records. See  
 9 United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008). And numerous federal courts have  
 10 now applied these longstanding constitutional principles to deny motions to suppress cell-site  
 11 records. See United States v. Madison, 2012 WL 3095357 at \*7-\*9 (S.D. Fla. July 30, 2012);  
 12 United States v. Graham, 846 F. Supp. 2d 384, 403-05 (D. Md. 2012); United States v. Dye,  
 13 2011 WL 1595255, at \*9 (N.D. Ohio April 27, 2011); United States v. Velasquez, 2010 WL  
 14 4286276, at \*5 (N.D. Cal. Oct. 22, 2010); United States v. Benford, 2010 WL 1266507, at \*3  
 15 (N.D. Ind. Mar. 26, 2010); United States v. Suarez-Blanca, 2008 WL 4200156, at \*8-\*11 (N.D.  
 16 Ga. Mar. 26, 2008).

17 C. Compulsory Process Is Subject To A Reasonableness Requirement, Not A  
 18 Warrant Requirement.

19 The compelled disclosure of business records in this case is supported not only by Miller  
 20 and Smith v. Maryland, but also by the more general law applicable to subpoenas. The subpoena  
 21 power is “the authority to command persons to appear and testify or to produce documents or  
 22 things.” In re Subpoena Duces Tecum, 228 F.3d 341, 346 (4th Cir. 2000). A 2703(d) order  
 23 functions as a judicial subpoena. It compels the recipient to produce specified information; the  
 24 recipient may move to quash; and it remains at all times under the supervision of the issuing  
 25 court. See 18 U.S.C. § 2703(d). Thus, cases addressing the Fourth Amendment principles  
 26 applicable to subpoenas also apply to 2703(d) order. Under these cases, no warrant or showing  
 27 of probable cause is required to use a subpoena to compel disclosure of non-privileged evidence  
 28 relevant to a criminal investigation.

1 A 2703(d) order may be used to compel disclosure of business records because the Fourth  
2 Amendment allows the United States to use a subpoena to compel disclosure of information  
3 relevant to a criminal investigation. By its terms, the Fourth Amendment protects people against  
4 unreasonable searches and seizures, but it imposes a probable-cause requirement only on the  
5 issuance of warrants. See U.S. Const. amend. IV (“and no Warrants shall issue, but upon  
6 probable cause”). The Supreme Court has explicitly rejected a probable-cause standard for  
7 subpoenas: “the Government cannot be required to justify the issuance of a grand jury subpoena  
8 by presenting evidence sufficient to establish probable cause because the very purpose of  
9 requesting the information is to ascertain whether probable cause exists.” United States v.  
10 R Enterprises, Inc., 498 U.S. 292, 297 (1991).

11 Instead of a probable cause standard, the Supreme Court has repeatedly held that under  
12 the Fourth Amendment, subpoenas must satisfy only a reasonableness standard. For example,  
13 in Wilson v. United States, 221 U.S. 361, 376 (1911), the Court held that “there is no  
14 unreasonable search and seizure when a [subpoena], suitably specific and properly limited in its  
15 scope, calls for the production of documents which, as against their lawful owner to whom the  
16 writ is directed, the party procuring its issuance is entitled to have produced.” The Court  
17 affirmed this rule in Oklahoma Press Publishing Co. v. Walling, 327 U.S. 186, 208 (1946), when  
18 it held that “the Fourth [Amendment], if applicable [to a subpoena], at the most guards against  
19 abuse only by way of too much indefiniteness or breadth in the things required to be ‘particularly  
20 described,’ if also the inquiry is one the demanding agency is authorized by law to make and the  
21 materials specified are relevant. The gist of the protection is in the requirement, expressed in  
22 terms, that the disclosure sought shall not be unreasonable.” See also United States v. Palmer,  
23 536 F.2d 1278, 1281-82 (9th Cir. 1976) (“Palmer also contends that his fourth amendment rights  
24 were violated because he had a reasonable expectation of privacy in the items subpoenaed. We  
25 do not explore the issue of a reasonable expectation of privacy, however, because the use of a  
26 properly limited subpoena does not constitute an unreasonable search and seizure under the  
27 fourth amendment. . . . The standard for a subpoena is reasonableness.”); Paine v. McCarthy, 527  
28

1 F.2d 173, 177 (9th Cir. 1975) (“[a] reasonable court order to produce evidence ... is not a search  
 2 or seizure within the meaning of the fourth amendment.”). Thus, despite defendant’s arguments  
 3 to the contrary, the United States was not required to obtain a warrant to compel disclosure of  
 4 historical business records in this case.

5 The subpoena power is grounded in the long-standing principle that the government has  
 6 the right to every witness’s testimony. The Supreme Court has repeatedly confirmed that “‘the  
 7 public . . . has a right to every man’s evidence,’ except for those persons protected by a  
 8 constitutional, common-law, or statutory privilege.” Branzburg v. Hayes, 408 U.S. 665, 688  
 9 (1972). The principle has remarkably deep roots. The Supreme Court has traced it to as early  
 10 as 1562 and held that it “was considered an ‘indubitable certainty’ that ‘cannot be denied’ by  
 11 1742.” Kastigar v. United States, 406 U.S. 441, 443 (1972) (citing Statute of Elizabeth, 5 Eliz.  
 12 1, c. 9, s. 12 (1562) and “parliamentary debate on the Bill to Indemnify Evidence, particularly  
 13 the remarks of the Duke of Argyle and Lord Chancellor Hardwicke, reported in 12 T. Hansard,  
 14 Parliamentary History of England 675, 693 (1812).”). Under this principle, the United States  
 15 has the right to compel disclosure of the cell-site records, IP address records, and security system  
 16 records because it has the right to every person’s evidence and because the records are evidence  
 17 relevant and material to a criminal investigation.

18 Thus, defendant cannot demonstrate a privacy interest in the material, and he cannot show  
 19 that the United States’ actions to obtain them were unreasonable. He therefore has no Fourth  
 20 Amendment challenge to their use.

21 D. Even If The Records Were Improperly Obtained, Suppression Is Not An  
 22 Appropriate Remedy.

23 Even if the records were improperly obtained, suppression is not an appropriate remedy.  
 24 In Weeks v. United States, the Supreme Court adopted the exclusionary rule for evidence  
 25 unlawfully seized in violation of the Fourth Amendment. See 232 U.S. 383 (1914). Suppression  
 26 of evidence, however, is the Court’s last resort rather than its first impulse, because the  
 27 exclusionary rule generates concomitant social costs by hindering the successful prosecution of  
 28 dangerous criminals. Hudson v. Michigan, 547 U.S. 586, 591 (2006); United States v. Leon, 468

1 U.S. 897, 907 (1984). Therefore, courts have been “cautio[us] against expanding” the  
2 exclusionary remedy, Colorado v. Connelly, 479 U.S. 157, 166 (1986), and have likewise  
3 rejected “[i]ndiscriminate application” of the rule. Leon, 468 U.S. at 908. The mere fact that a  
4 constitutional violation has occurred does not necessitate suppression of the evidence thereby  
5 obtained; instead, “[w]hether the exclusionary sanction is appropriately imposed in a particular  
6 case . . . is ‘an issue separate from the question whether the Fourth Amendment rights of the  
7 party seeking to invoke the rule were violated by police conduct.’” Leon, 468 U.S. at 906  
8 (quoting Illinois v. Gates, 462 U.S. 213, 223 (1983)). Suppression should be employed only  
9 where the remedial objectives of the exclusionary rule are “efficaciously served”—i.e., where  
10 the prospect of exclusion to deter wrongful police conduct outweighs the substantial costs to  
11 society of potentially letting guilty defendants go free. United States v. Calandra, 414 U.S. 338,  
12 348 (1974).

13       Suppression is a particularly inappropriate remedy for violations of 18 U.S.C. § 2703, the  
14 Stored Communications Act (SCA). “The remedies and sanctions described in [the SCA, 18  
15 U.S.C. §§ 2701-2712] are the only judicial remedies and sanctions for nonconstitutional  
16 violations of [the SCA].” 18 U.S.C. § 2708; See also United States v. Smith, 155 F.3d 1051,  
17 1056 (9th Cir. 1998) (“[T]he Stored Communications Act does *not* provide an exclusion remedy.  
18 It allows for civil damages . . . and criminal punishment . . . but nothing more.”) (citations  
19 omitted).

20       Defendant argues that the evidence should be suppressed because the subpoenas and 18  
21 U.S.C. § 2703(d) court order were insufficiently particular. (Mot. at 328-29.) Defendant cites  
22 no authority suggesting that lack of particularity is a basis for suppressing information obtained  
23 through a subpoena or 2703(d) order.

24       Moreover, suppression would be inappropriate because here law enforcement acted in  
25 good faith reliance on case law, statutes, and court orders. See, e.g., Davis v. United States, 131  
26 S. Ct. 2419 (2011) (good faith reliance on case law); Illinois v. Krull, 480 U.S. 340 (1987) (good  
27 faith reliance on statute); United States v. Leon, 468 U.S. 897 (1984) (good faith reliance on  
28

warrant). For example, in United States v. Warshak, 631 F.3d 266, 288-92 (6<sup>th</sup> Cir. 2010), the Sixth Circuit held that the government violated the Fourth Amendment when it used a 2703(d) order to compel disclosure of the content of email from a commercial ISP, but it relied on Krull to hold that the exclusionary rule did not apply. In sum, the third-party doctrine of United States v. Miller and Smith v. Maryland has been consistently applied by courts since the 1970s, 18 U.S.C. § 2703(d) permits law enforcement to obtain IP address and cell site records without a warrant, and the United States relied on court orders and subpoenas to obtain the relevant material. There is no wrongful police conduct to deter, and therefore no basis for suppression.

2. The Government's Efforts To Locate The Aircard Pursuant To The Tracking Warrant Were Reasonable.

Defendant also challenges the United States' actions during the real-time aircard location operation on July 16, 2008. The United States obtained two Orders, CR 08-90330MISC and CR 08-90331MISC, but has agreed per the Government's Memorandum Re Motion for Discovery (CR 674) to rely on Order CR 08-90330MISC for the FBI's use of the equipment to locate Aircard. The United States has agreed that the Court can assume, for purposes of the Motion to Suppress, that the FBI's use of location equipment, including cell site simulators that can be operated in a vehicle on or foot, constituted a search and seizure under the Fourth Amendment. (CR 674.) As explained below, the tracking warrant authorized the FBI to locate the aircard, and they executed the warrant reasonably.

A. The FBI Located Defendant's Aircard Pursuant To A Warrant Based On Probable Cause.

The tracking warrant at issue, CR 08-90330MISC, properly authorized the United States to locate defendant's aircard. The Fourth Amendment states that search warrants may be issued only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." U.S. Const. Amend. IV. As the Supreme Court has emphasized, this language "require[s] only three things": a warrant must be issued by a neutral magistrate, it must be based on a showing of "probable cause to believe that 'the evidence sought will aid in a particular apprehension or conviction' for a particular offense,"

1 and it must satisfy the particularity requirement. Dalia v. United States, 441 U.S. 238, 255  
2 (1979). The warrant here, which authorized the government to determine the location of  
3 defendant's aircard, satisfies these three requirements.

4 First, the warrant was issued by United States Magistrate Judge (now District Judge)  
5 Richard Seeborg, a neutral magistrate, on July 11, 2008.

6 Second, Judge Seeborg found that the warrant established "probable cause to believe that  
7 the use and monitoring of a mobile tracking device" for defendant's aircard "will lead to  
8 evidence of violations" of specified crimes, "as well as to the identification of individuals who  
9 are engaged in the commission of these offenses." Warrant CR-08-90330 at 2. This finding is  
10 amply supported by the seventeen page affidavit of Special Agent William Ng. The affidavit  
11 stated that the United States sought to use a device "to ascertain the physical location of [the  
12 defendant's aircard]," described defendant's elaborate fraud scheme and techniques to evade  
13 apprehension, connected defendant's aircard to use in the fraud scheme, and explained that the  
14 equipment the government sought to use "ultimately generate[s] a signal that fixes the  
15 geographic position" of the aircard. Affidavit for Warrant CR-08-90330 at ¶ 1, ¶ 3, ¶ 34 and ¶  
16 42. Thus, the United States demonstrated "probable cause to believe that the use and monitoring  
17 of the equipment would lead to evidence of the subject violations and the identification of the  
18 individuals who were engaged in the commission of the offenses. Warrant CR-08-90330 at 2.

19 Third, the warrant described with particularity the item to be located: "The Verizon  
20 Wireless broadband access card/cellular telephone assigned Telephone Number (415)264-9596  
21 and Electronic Serial Number (ESN) 005-00717190 (the Target Broadband Access Card/Cellular  
22 Telephone)." Warrant CR-08-90330 at 1. It also described with particularity the duration of the  
23 authorized tracking: "a period not to exceed thirty (30) days." Warrant CR-08-90330 at 2. It  
24 ordered monitoring transmissions related to defendant's aircard, "limited to transmissions needed  
25 to ascertain the physical location" of the aircard. Warrant CR-08-90330 at 3.

26 Defendant's numerous objections to the warrant are without merit. First, defendant  
27 argues that the execution exceeded the scope because the warrant did not specifically authorize  
28



the FBI to use a cell site simulator and that the actions authorized by the warrant “were not supported by an applicable finding of probable cause.” (Mot. at 292-96, 301-302). For example, he complains that the warrant did not list “the electricity being provided to the aircard.” (Mot. at 294.) These objections fundamentally misunderstand the warrant requirement: the warrant must establish probable cause that locating the Aircard will lead to evidence of crime or apprehension of criminals, and it must specify what is to be located (the Aircard), but it need not specify how the Aircard is to be located or what actions will be taken to locate the Aircard.

In Dalia v. United States, the Supreme Court rejected the notion that a warrant must precisely describe the manner of its execution. 441 U.S. 238, 257 (1979). In Dalia, the government obtained a wiretap order to intercept the defendant’s oral conversations in his law office. Id. at 242. To execute the order, FBI agents broke into his office at midnight and spent three hours installing a listening device; approximately 40 days later they entered again to remove the device. Id. at 245. At trial, Dalia challenged the United States’ use of the intercepted communications because the wiretap order itself did not authorize the covert entry. Id. The district court rejected this argument, and the Supreme Court agreed:

Nothing in the language of the Constitution or in this Court’s decisions interpreting that language suggests that, in addition to the three requirements discussed above, search warrants also must include a specification of the precise manner in which they are to be executed. On the contrary, it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant—subject of course to the general Fourth Amendment protection “against unreasonable searches and seizures.”

... [Dalia’s] view of the Warrant Clause parses too finely the interests protected by the Fourth Amendment. Often in executing a warrant the police may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant. For example, police executing an arrest warrant commonly find it necessary to enter the suspect’s home in order to take him into custody, and they thereby impinge on both privacy and freedom of movement. Similarly, officers executing search warrants on occasion must damage property in order to perform their duty.

Id. at 257-258.

Moreover, to the extent that the warrant itself was unclear, the application and supporting affidavit clearly show what the FBI intended to do: use mobile tracking equipment to find the

1 aircard. Compare CR 08-90330MISC (tracking warrant) at 1 (“This matter is before the Court  
2 pursuant to an Application . . . .”) with United States v. SDI Future Health, 568 F.3d 684, 699-  
3 700 (9th Cir. 2009) (holding that language “noting ‘the supporting affidavit(s)’ as the ‘grounds  
4 for application for issuance of the search warrant’” is sufficient to incorporate the affidavit by  
5 reference).

6 Defendant makes several arguments that the warrant is lacking in particularity, but these  
7 arguments are based on a misunderstanding of the particularity requirement for warrants. He  
8 argues that the “mobile tracking device” term lacks particularity, that the description of the place  
9 to be searched lacks particularity, and that the “all data, information, facilities, and technical  
10 assistance” phrase lacks particularity. (Mot. at 297-300, 302-303.) “The Fourth Amendment,  
11 however, does not set forth some general ‘particularity requirement.’ It specifies only two  
12 matters that must be ‘particularly describ[ed] in the warrant: ‘the place to be searched’ and ‘the  
13 persons or things to be seized.’” United States v. Grubbs, 547 U.S. 90, 97 (2006). Thus, the  
14 particularity requirement simply does not extend to the definition of “mobile tracking device”  
15 or the warrant’s technical assistance provision, as these concern how the warrant is to be  
16 executed, not the place to be searched or the person or things to be seized. It is true that the  
17 warrant does not describe the place to be searched, as the whole purpose of the warrant was to  
18 determine the then unknown location of the Aircard. But as the Supreme Court explained in the  
19 tracking device case United States v. Karo, 468 U.S. 705, 718 (1984), a warrant to locate an item  
20 need not specify the place to be searched:

21 The Government contends that it would be impossible to describe the “place” to  
22 be searched, because the location of the place is precisely what is sought to be  
23 discovered through the search. However true that may be, it will still be possible  
24 to describe the object into which the beeper is to be placed, the circumstances that  
led agents to wish to install the beeper, and the length of time for which beeper  
surveillance is requested. In our view, this information will suffice to permit  
issuance of a warrant authorizing beeper installation and surveillance.

25 468 U.S. at 718. The government here satisfied these Karo requirements, so the warrant here  
26 satisfies the Fourth Amendment.

1        Moreover, the execution of the warrant was reasonable. The touchstone of Fourth  
2 Amendment jurisprudence has always been reasonableness, “which is measured in objective  
3 terms by examining the totality of the circumstances.” Ohio v. Robinette, 519 U.S. 33, 34  
4 (1996); Samson v. California, 547 U.S. 843, 848 (2006); United States v. Knights, 534 U.S. 112,  
5 118 (2001).

6        Defendant makes numerous allegations in his motion about what the United States did  
7 to locate his aircard — e.g., that it used triangulation techniques, drained power (a minute  
8 amount by any estimate) from the laptop, wrote data to the aircard, and interrupted his internet  
9 connection. (Mot. at 261-282.) Allegations in a motion are not evidence, though, see, e.g.,  
10 United States v. Zermeno, 66 F.3d 1058, 1062 (9<sup>th</sup> Cir. 1995), and defendant has not shown that  
11 he is qualified to offer expert opinion testimony on these matters. Presumably he will present  
12 expert testimony at a suppression hearing in an attempt to prove his allegations.

13        Even if the United States did all of these things, the execution of the warrant would still  
14 be reasonable. Moreover, the United States did not do a number of the things defendant has  
15 alleged. Defendant was perpetrating a multi-million-dollar tax fraud scheme, and he hid his  
16 tracks through the use of encrypted e-mails, money mules, layers of false identities, forged  
17 documents, forged identification cards, and botnets and/or proxies. He also advised, via  
18 encrypted e-mails, that he was interested in procuring a machinegun armed with a silencer and  
19 would send armed couriers to cash pick-ups who would readily shoot people at the scene if  
20 things did not go as planned. The alleged inconvenience and intrusiveness of the aircard  
21 location operation (which went undetected by an individual who appeared to spend a significant  
22 portion every day seeking to avoid detection or identification) was reasonable under the  
23 circumstances. See, e.g., Los Angeles County v. Rettele, 550 U.S. 609, 611 (2007) (officers  
24 acted reasonably, even though they executed warrant at a home the suspects had left months  
25 before and ordered naked, sleeping residents out of bed at gunpoint); Avina v. United States, 681  
26 F.3d 1127, 1129 (9<sup>th</sup> Cir. 2012) (officers acted reasonably, even though they knocked down front  
27 door with battering ram, entered with guns drawn, and forcefully pushed occupant to ground and  
28

1 handcuffed him); United States v. Ankeny, 502 F.3d 829, 833 (9<sup>th</sup> Cir. 2007) (officers acted  
2 reasonably, even though 44 armed officers executed warrant at 5:30 a.m., used battering ram on  
3 front door, threw multiple flash-bangs that gave occupant first- and second-degree burns and set  
4 fire to bed, shot out ten windows, and caused extensive damage to home); United States v.  
5 Becker, 929 F.2d 442, 444 (9<sup>th</sup> Cir. 1991) (officers acted reasonably, even though they rented  
6 jackhammer to remove portions of the concrete slab to look for drugs); see also United States  
7 v. Dalia, 441 U.S. 238, 257-58 (“[O]fficers executing search warrants on occasion must damage  
8 property in order to perform their duty.”). The Supreme Court “has ‘repeatedly refused to  
9 declare that only the least intrusive search practicable can be reasonable under the Fourth  
10 Amendment.’” City of Ontario v. Quon, 130 S. Ct. 2619, 2632 (2010). But it is noteworthy that  
11 defendant does not suggest that the United States could have located him through less intrusive  
12 means. As the Sixth Circuit recently explained, “[w]hen criminals use modern technological  
13 devices to carry out criminal acts and to reduce the possibility of detection, they can hardly  
14 complain when the police take advantage of the inherent characteristics of those devices to catch  
15 them.” United States v. Skinner, \_\_\_ F.3d \_\_\_, 2012 WL 3289801, at \*1 (6<sup>th</sup> Cir. Aug. 14,  
16 2012).

17 Defendant complains that the tracking warrant did not comply with the return and notice  
18 requirements in Federal Rule of Criminal Procedure 41(f)(2). (Mot. at 304-306.) He is right.  
19 The warrant stated (albeit perhaps improperly) that the agents were not required to make a return  
20 or serve a copy of the warrant on the person whose property was located. Nevertheless,  
21 suppression is not an appropriate remedy for a failure to make a return or serve a copy of the  
22 warrant, or for other technical violations. See United States v. Hector, 474 F.3d 1150, 1155 (9<sup>th</sup>  
23 Cir. 2007) (holding that suppression is inappropriate remedy for failure to serve copy of search  
24 warrant); United States v. Motz, 936 F.2d 1021, 1025 (9<sup>th</sup> Cir. 1991) (holding that where  
25 defendants "were not prejudiced by the agents' failure to perform the ministerial requirements"  
26 of return and inventory, "[t]he district court was correct in refusing to suppress the evidence");  
27 United States v. Hall, 505 F.2d 961, 963 (3<sup>rd</sup> Cir. 1974) (holding that suppression is  
28

1 inappropriate remedy for failure to make return). Defendant claims that he would have fled if  
2 he knew law enforcement was tracking his aircard (Mot. CR 824-2 (Rigmaiden Dec.) at 4 ¶ 14),  
3 but the United States could have sought delayed notice for precisely that reason. See 18 U.S.C.  
4 § 3103a(b)(1). Thus, the United States would have obtained the location of defendant's aircard  
5 even if it did not commit these technical violations, and the Supreme Court has held that "but-for  
6 causality" is a necessary condition for suppression. See Hudson v. Michigan, 547 U.S. 586, 592  
7 (2006). Moreover, in this case the agents had no real opportunity to serve the owner of the  
8 aircard with a copy of the tracking warrant; defendant obtained it using a false identity, a non-  
9 existent address, and a driver's license number assigned to someone else. Furthermore, there  
10 was a statutory basis for the magistrate judge's order regarding notice. The warrant was issued  
11 in part under 18 U.S.C. § 2703. Warrant CR-08-90330 at 1. Because it is a warrant to obtain  
12 non-content information associated with a customer or subscriber of an electronic  
13 communication service, it is a warrant under § 2703(c)(1). Although § 2703(c)(1) warrants are  
14 in most respects like Rule 41 warrants (they are "issued using the procedures described in" Rule  
15 41), § 2703 specifies a few differences from the procedures of Rule 41. Significantly, 18 U.S.C.  
16 § 2703(c)(3) specifies that "[a] governmental entity receiving records or information under this  
17 subsection is not required to provide notice to a subscriber or customer."

18 Finally, defendant argues that the United States destroyed data generated by the FBI  
19 during the aircard tracking operation in bad faith, warranting suppression of all evidence. (CR  
20 830-2 at 1.) The failure to preserve exculpatory evidence can violate a defendant's due process  
21 rights, but the evidence must "possess an exculpatory value that was apparent before the  
22 evidence was destroyed, and be of such a nature that the defendant would be unable to obtain  
23 comparable evidence by other reasonably available means." California v. Trombetta, 467 U.S.  
24 479, 489 (1984). If the evidence is only potentially useful, a defendant must show that the  
25 government acted in bad faith. Arizona v. Youngblood, 488 U.S. 51, 58 (1988).

26 Defendant speculates that the destroyed data might confirm some of his allegations of  
27 what the United States did to locate his aircard, but this is (1) mere speculation (2) about material  
28

1 that would not even be evidence at trial, (3) that would not demonstrate that the government  
 2 acted unreasonably in executing the warrant, (4) that was required by the warrant to be  
 3 expunged, and (5) that would have been destroyed pursuant to valid and reasonable FBI policy  
 4 in any event. He also claims that it was done in bad faith, but he provides no proof. The FBI  
 5 destroyed the data because it was not evidence and because FBI policy requires agents to clear  
 6 the equipment of data prior to each operation. Defendant's wild conspiracy theories fail to  
 7 demonstrate any basis for suppression. Cf. Trombetta, 467 U.S. at 490 (no due process violation  
 8 in DUI prosecution because "chances are extremely low that preserved [breath] samples would  
 9 have been exculpatory"); United States v. Flyer, 633 F.3d 911, 916 (9<sup>th</sup> Cir. 2011) (no due  
 10 process violation in child pornography prosecution when FBI accidentally corrupted data on  
 11 defendant's computer); Phillips v. Woodford, 267 F.3d 966, 987-88 (9<sup>th</sup> Cir. 2001) (no due  
 12 process violation in murder prosecution when police destroyed murder victim's car); Cooper v.  
 13 Calderon, 255 F.3d 1104, 1113-14 (9th Cir. 2001) (no due process violation in murder  
 14 prosecution when police destroyed bloody overalls turned in by witness).

15 B. Defendant Cannot Show That His Expectation Of Privacy In The Location Of An  
 16 Aircard Procured By Fraud And Used To Commit Crime Was Objectively  
Reasonable.

17 To establish a Fourth Amendment violation, defendant must first prove that he had a  
 18 genuine expectation of privacy in the place searched or the items seized, and that such an  
 19 expectation was one that society is prepared to recognize as reasonable. Rakas v. Illinois, 439  
 20 U.S. 128, 143 (1978). In satisfying this burden, a legitimate expectation of privacy means more  
 21 than the belief, "however well justified, that certain facts will not come to the attention of the  
 22 authorities." United States v. Jacobsen, 466 U.S. 109, 122 (1984). Only searches and seizures  
 23 that infringe upon the former implicate the Fourth Amendment. Id. Here, defendant is unable  
 24 to demonstrate his expectation of privacy in the location of his aircard, as stated above, a device  
 25 fraudulently purchased and maintained under the identity of another living person, and stored  
 26 in an apartment fraudulently obtained and maintained under the identity of a second deceased  
 27 person, was objectively reasonable. In this case, nothing could have stopped the true Travis  
 28

1 Rupard carrying a copy of his Social Security Card, from gaining access to the Aircard's  
2 account. Therefore, even if the Court concludes that the search or seizure exceeded the scope  
3 of the tracking device warrant or was otherwise defective, there is no evidence that defendant's  
4 constitutional rights were breached, nor should he be afforded any under the circumstances of  
5 his possession and operation of the Aircard.

6 Defendant contends that he manifested a subjective expectation of privacy in his  
7 apartment, as well as in the laptop computer and aircard contained therein. Memorandum Re:  
8 Fourth Amendment Violations at 208, United States v. Rigmaiden, (No. CR08-814-PHX-DGC).  
9 Defendant presents no evidence, however, that establishes that society is prepared to recognize,  
10 or should even seriously consider, that expectation as objectively reasonable. The Fourth  
11 Amendment should not shield a defendant from the search of property obtained by fraud, and  
12 defendant openly concedes he both rented his apartment and purchased his computer under an  
13 alias. Id. at 205, 210. In United States v. Caymen, the Ninth Circuit held that the defendant had  
14 failed to establish a legitimate expectation of privacy in the contents of a laptop that he had  
15 purchased using a stolen credit card. 404 F.3d 1196 (9th Cir. 2005). The court reasoned, "The  
16 Fourth Amendment does not protect a defendant from a warrantless search of property that he  
17 stole, because regardless of whether he expects to maintain privacy in the contents of the stolen  
18 property, such an expectation is not one that society is prepared to accept as reasonable." Id.  
19 But see United States v. Cunag, 386 F.3d 888 (9th Cir. 2004) ("[I]n the Ninth Circuit, the rule  
20 is that even if the occupant of a hotel room has procured that room by fraud, the occupant's  
21 protected Fourth Amendment expectation of privacy is not finally extinguished until the hotel  
22 justifiably takes 'affirmative steps to repossess the room.'").

23 There is no reason to distinguish property obtained by fraud from property stolen by  
24 robbery or trespass. In United States v. Johnson, for example, the court found that the defendant  
25 had no reasonable expectation of privacy in a storage container rented by the defendant's  
26 girlfriend using a stolen identity. 584 F.3d 995 (10th Cir. 2009). The defendant in Johnson  
27 attempted to distinguish Caymen on the grounds that there was no evidence that a fraudulent  
28



1 means of payment was used to rent the storage locker, an argument Rigmaiden also raises in his  
 2 Motion (without ever identifying the origin of the funds). Id. at 1002-03; Motion re: Fourth  
 3 Amendment Violations at 211, Rigmaiden, (No. CR08-814-PHX-DGC). Nevertheless, the  
 4 Tenth Circuit explicitly rejected this logic: it explained that a “fraud” occurred notwithstanding  
 5 the defendant’s lawful payment of rent for the unit because his use of a third party’s identity  
 6 constituted a material misrepresentation to the storage company; thus, “the reasonableness of any  
 7 privacy expectations [the defendant] might have had were undermined by his . . . decision to use  
 8 [a stolen] identity” to obtain the unit. Id. at 1001-02. The court acknowledged that the “ultimate  
 9 question of whether a privacy expectation is reasonable is a value judgment,” and it concluded  
 10 that whatever interest the defendant might have had in the storage locker was not the kind of  
 11 interest the Fourth Amendment was intended to protect. Id. at 1001, 1004 (quoting WAYNE R.  
 12 LAFAVE, Search and Seizure: A Treatise on the Fourth Amendment § 2.1(d) at 443 (4th ed.  
 13 2004)). The court declared it would “not be a party to th[e] fraud by legitimizing [the  
 14 defendant]’s interest in the storage unit.” Id.

15 Moreover, courts have repeatedly found that defendants lack standing to challenge  
 16 searches of items that are registered or addressed to a fictitious name, explaining that defendants  
 17 abandoned their objective expectation of privacy by using a false identity. See, e.g., United  
 18 States v. Lozano, 623 F.3d 1055, 1062-63 (9th Cir. 2010) (O’Scannlain, J., concurring) (citing  
 19 cases from the Fifth, Seventh, and Eighth Circuits for the principles that a defendant has no  
 20 “legitimate expectation of privacy in mail addressed to his public alias when that alias was used  
 21 solely in a criminal scheme” and that “‘wrongful’ interests do not give rise to legitimate  
 22 expectations of privacy.”); United States v. Pitts, 322 F.3d 449 (7th Cir. 2003) (Evans, J.,  
 23 concurring); United States v. Daniel, 982 F.2d 146 (5th Cir. 1993); United States v. Lewis, 738  
 24 F.2d 916, 920 n.2 (8th Cir. 1984); United States v. Davis, No. 10-339-HA, 2011 WL 2036463,  
 25 at \*2-3 (D. Or. May 24, 2011) (“Although an individual may have a subjective expectation of  
 26 privacy in property that is attached to a fictitious name, that is not a privacy interest that society  
 27 recognizes as reasonable.”); United States v. Coverson, No. 3:9-CR-00075-TMB-DMS, 2011  
 28

1 WL 1044632, at \*4-5 (D. Alaska Mar. 22, 2011) (holding that defendant had no reasonable  
2 expectation of privacy in a package addressed to the defendant's alias, a fictitious name "used  
3 for a one-time purpose . . . to further a criminal scheme"); United States v. Suarez-Blanca, No.  
4 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at \*6-7 (N.D.Ga. Apr. 21, 2008) ("The use of a  
5 fictitious name or names of a third party indicates that [the defendant] does not have a privacy  
6 interest."). In this case, the aircard was registered with Verizon Wireless to "Travis Rupard,"  
7 a different living person, while defendant simultaneously rented and used the apartment and  
8 electricity obtained via a second fraudulent identity, the deceased "Steven Brawner," and  
9 operated the laptop via a third fraudulent identity "Andrew Johnson."

10 This not a situation where an individual, such as an author, has a lawful reason for using  
11 a nom de plum. See Pitts, 322 F.3d at 461. The herculean extent of defendant's efforts to  
12 conceal his true identity makes it exceedingly clear that "Travis Rupard" was truly the fraudulent  
13 assumption of another person's identity which defendant used to conceal his location and  
14 ongoing criminal enterprise. Nor is this case like United States v. Villarreal or United States v.  
15 Richards, two Fifth Circuit cases not cited by defendant but which support his position that the  
16 use of aliases does not necessarily preclude the assertion of a Fourth Amendment violation,  
17 because unlike those cases defendant has no publicly-established connection to his alias. In  
18 Richards, the defendant was the owner of a company to which a package of heroin was  
19 addressed, and on the that basis the Fifth Circuit found that the defendant had sufficient standing  
20 to challenge officers' warrantless opening of the box. 638 F.2d 765, 769-770 (5th Cir. 1981).  
21 Similarly, in Villarreal the defendant was known by at least one witness by the fictitious name  
22 connected to two shipping drums full of marijuana that Customs agents opened without court  
23 authorization. 963 F.2d 770, 772-73 (5th Cir. 1992). Conversely, defendant went to great  
24 lengths to have no public connection to "Travis Rupard" or any of his other aliases, so it follows  
25 that he does not have a legitimate expectation of privacy in the broadband access card registered  
26 in Rupard's name. See Lozano, 623 F.3d at 1064 (O'Scannlain, J., concurring).

1 Finally, defendant's reliance on United States v. Issacs for the precept that his reasonable  
2 expectation of privacy in his apartment extended also to the laptop and aircard is misplaced. In  
3 Issacs, Secret Service agents found several journals inside the defendant's safe marked up with  
4 notions related to repeated drug transactions. 708 F.2d 1365, 1366 (9th Cir 1983). The  
5 defendant was convicted of possession with intent to distribute based on the evidence in the  
6 journals, which the court admitted despite the defendant's motion to suppress. Id. On appeal,  
7 the government contended that the defendant's disclaimer of ownership at trial precluded his  
8 efforts to contest the admission of the books, even though it had previously argued that the  
9 defendant's possession of the journals demonstrated his guilt for the alleged offenses. Id. at  
10 1367-68. The Ninth Circuit found this "distinction the government [sought] to draw. . .  
11 untenable," and the court held that the government could not simultaneously charge possession  
12 and dispute the defendant's expectation of privacy when the underlying facts made such  
13 positions "necessarily inconsistent." Id. at 1368.

14 Here, the defendant is attempting to capitalize on the government's concession that the  
15 defendant was the actual occupant of the apartment to prove by proxy that he had a legitimate  
16 privacy interest in the Aircard found there. The government has never conceded that defendant  
17 had a valid expectation of privacy in anything that he had obtained, possessed, or maintained  
18 through the use of a fraudulent identity; what it has maintained is simply that he personally  
19 possessed, obtained, or maintained the items. In this case there is no allegation that the  
20 government is contradicting a prior finding of fact. The Ninth Circuit was troubled in Issacs by  
21 what it perceived to be the government's discrepant positions on appeal, arguing on one hand  
22 that the defendant's denial of ownership at trial foreclosed a Fourth Amendment challenge to  
23 the search and seizure of the journals but, on the other, that the defendant possessed the ledger  
24 for purposes of guilt. See Issacs, 708 F.2d at 1368. There is no question here that the defendant  
25 purchased the Aircard and maintained the account through the assumption and false use of the  
26 identity of another, defendant also spends several pages of his Motion articulating his possessory  
27 and property interests in it. See Motion re: Fourth Amendment Violations at 197-98, Rigmaiden,

(No. CR08-814-PHX-DGC). However, it is well established that “while property ownership is clearly a factor to be considered in determining whether an individual’s Fourth Amendment rights have been violated, property rights are neither the beginning nor the end of this Court’s inquiry” because possession does not “invariably represent the protected Fourth Amendment interest.” United States v. Salvucci, 448 U.S. 83, 91 (1980); see also United States v. Karo, 468 U.S. 705, 722 (1984) (O’Connor, J., concurring) (“A privacy interest in . . . a closed container that enters a home with the homeowner’s position cannot be inferred mechanically by reference to the more general privacy interests in the home itself.”). Thus, there is nothing inconsistent about the government’s position that defendant had physical possession of the aircard and maintained the account, yet was not subject to a Fourth Amendment deprivation when it was searched. Even under Issacs defendant must still put forth a factual predicate that he had a legitimate expectation of privacy in the aircard itself.

Society has no interest in protecting the Aircard in this case from a warrantless search. On the contrary, society's interests would be better served by a policy that gave no protection to the privacy interests of individuals in defendant's position, a thief and fugitive who concealed his true identity and location in order to operate a sophisticated and complex tax fraud scheme with a fraudulently obtained Aircard, apartment and laptop, and regularly invaded the computers, privacy and financial records of innocent victims. Whatever subjective privacy expectations defendant had in the Aircard are not justifiable, and, thus, the agents in this case were not required to obtain a warrant to search the device.

C. Defendant Did Not Have Reasonable Expectation of Privacy In The Area Immediately Outside Of The Apartment He Occupied.

Particularly with respect to the operation of equipment by the FBI during the Aircard mission, defendant appears to contends that he had a reasonable expectation of privacy in the common areas around the apartment he occupied due to the overall security features of complex. See Declaration Under Penalty of Perjury (824-2) at 1, ¶ 2, and Motion (CR 824-1) at 204. The Ninth Circuit is quite clear that occupants of multi-unit apartment complexes with common hallways, staircases, doorways, etc., do not enjoy a reasonable expectation of privacy outside

1 of their own units regardless of extensive security features. See, United States v. Nohara, 3 F.3d  
2 1239, 44-41 (9th Cir. 1993) (The Ninth Circuit joined the First, Second, and Eighth Circuits  
3 which have rejected claims of expectations of privacy in common areas and held an apartment  
4 dweller has no reasonable expectation of privacy in the secured common areas of a building  
5 whether an officer trespasses or not.)

6 D. Suppression Is Not An Appropriate Remedy For Any Technical Deficiencies In  
7 The Warrant.

8 Finally, suppression would be an inappropriate remedy for any technical deficiencies in  
9 the warrant. The tracking warrant issued by U.S. Magistrate Judge (now District Judge) Richard  
10 Seeborg was similar to numerous cell phone tracking warrants issued across the United States  
11 by other U.S. magistrate judges, including U.S. magistrate judges here in the District of Arizona.  
12 The FBI located defendant's aircard after demonstrating to a U.S. magistrate judge that it had  
13 probable cause to believe that locating the aircard would lead to evidence of crime and the  
14 identification of the perpetrator. There was no wrongful police conduct, so there is no reason for  
15 suppression.

16 Suppression is inappropriate in this case under the reasoning of the concurring opinion  
17 of Judge Donald in United States v. Skinner, \_\_\_ F.3d \_\_\_, 2012 WL 3289801 (6th Cir. Aug.  
18 14, 2012). In Skinner, the United States obtained prospective GPS location information of a  
19 defendant's phone using a 2703(d) order; the Sixth Circuit held that the defendant had no  
20 reasonable expectation of privacy in that information. Id. at \*4. Judge Donald disagreed with  
21 the court regarding whether the defendant had a reasonable expectation of privacy; she stated  
22 that "officers should have obtained a warrant authorizing them to collect GPS real-time location  
23 information." Id. at \*14. Nevertheless, she held that suppression was not warranted based on  
24 United States v. Leon, 468 U.S. 897 (1984). She explained that "[t]here is no evidence that  
25 officers in this case engaged in any intentional misconduct; rather, it appears they made a  
26 procedural error." She further explained that "officers had probable cause to conduct the search,  
27 and the information establishing that probable cause was presented to the magistrate judge in the  
28 affidavits supporting the application for a court order." To the extent officers made procedural

1 errors in this case, Judge Donald's reasoning is equally applicable here. There is no evidence  
2 of intentional misconduct. Instead, agents were using a relatively new technology, and they  
3 faced a lack of legal precedent regarding the proper form of a warrant to obtain the location  
4 information they sought. Indeed, the agents in this case actually sought a warrant, and the  
5 affidavit made clear that it sought authorization "to ascertain the physical location" of  
6 defendant's aircard. Affidavit for Warrant CR-08-90330 at ¶ 1. In these circumstances, they  
7 were entitled to rely in good faith on the warrant to determine the location of defendant's aircard.

8 3. The Search Of Defendant's Apartment And Computer Pursuant To Search  
9 Warrant Was Reasonable.

10 Defendant also challenges the searches of his apartment and computer pursuant to search  
11 warrant. (CR 830-1.) As explained below, the United States conducted the searches pursuant to  
12 warrants issued by neutral U.S. magistrate judges based on a finding of probable cause, the  
13 searches were reasonable, and the agents acted in good faith. Accordingly, there is no reason to  
14 suppress any of the evidence obtained.

15 First, defendant argues that the second warrant to search his apartment was invalid,  
16 because the first warrant to search the same location had already been returned unexecuted. The  
17 second warrant was issued properly, after a U.S. magistrate judge again made a finding of  
18 probable cause to believe that the location would contain evidence of crime. See Sgro v. United  
19 States, 287 U.S. 206, 211 (1932) ("The new warrant must rest upon a proper finding and  
20 statement by the commissioner that probable cause then exists."). Defendant cites no authority  
21 for the striking proposition that law enforcement cannot seek a second warrant after the first is  
22 returned unexecuted. As stated above, the only reason the first warrant was not executed was  
23 because the agents did not want to tip off the yet-to-be-observed occupant of the apartment.

24 Second, defendant argues that the search warrant application failed to demonstrate  
25 probable cause. "Perhaps the central teaching of our decisions bearing on the probable cause  
26 standard is that it is a 'practical, nontechnical conception.' 'In dealing with probable cause, . .  
27 . as the very name implies, we deal with probabilities. These are not technical; they are the  
28 factual and practical considerations of everyday life on which reasonable and prudent men, not

1 legal technicians, act.’” Illinois v. Gates, 462 U.S. 213, 231 (1983) (finding probable cause based  
2 on corroborated anonymous tip) (quoting Brinegar v. United States, 338 U.S. 160, 175-76  
3 (1949)). Here, the affidavit, as set forth above in detail, explained that FBI, IRS and USPIIS  
4 agents traced the criminal activity to the Aircard located in defendant’s apartment complex, and  
5 found that the handwriting on the rental agreement for defendant’s apartment matched other  
6 documents tied to the scheme. (There were other indicia included in the search warrant affidavit,  
7 such as defendant’s use of a false identity, stolen driver’s license number, and fraudulent tax  
8 return in the rental application.) “[S]o long as the magistrate had a ‘substantial basis for ...  
9 conclud[ing]’ that a search would uncover evidence of wrongdoing, the Fourth Amendment  
10 requires no more.” Id. at 236. Even if the U.S. magistrate judge issued the search warrant in  
11 error, the FBI and IRS agents executed it in good faith. United States v. Leon, 468 U.S. 897  
12 (1984) (good faith reliance on warrant).

13 Third, defendant argues that the use of the key found on his person was a search regulated  
14 by the Fourth Amendment, Motion (CR 824-1) at 284-85, and later contends that the search was  
15 warrantless. Motion at 355. The agents clearly had authority to use the key in this case. As  
16 noted above, first, the key was located on defendant during a search incident to an arrest  
17 pursuant to a federal arrest warrant shortly after 4:15 p.m., on August 3, 2008; second, the agents  
18 were authorized by the rental company to access the apartment complex at that time; third, the  
19 agents had a sealed search warrant for the apartment in hand; and fourth, once the key was  
20 inserted into the lock and turned the lock, the unoccupied apartment was secured by the  
21 investigation team until the full entry and search teams were gathered and entry was made  
22 pursuant to the warrant at 5:20 p.m.

23 Fourth, defendant argues that the United States violated the terms of the search warrant  
24 by continuing to review digital material seized pursuant to the search warrant. To determine  
25 whether the execution of the search warrant was reasonable, the Court considers the totality of  
26 the evidence and not just whether the agents complied with all of the warrant’s explicit terms.  
27 See Richards v. Wisconsin, 520 U.S. 385, 395 (1997).



1 In Richards, the Supreme Court held that officers' unannounced entry into a defendant's  
2 motel room was reasonable under the Fourth Amendment, even though the magistrate judge had  
3 specifically refused to issue a "no-knock" warrant. Id. Writing for a unanimous Court, Justice  
4 Stevens explained that the defendant's unusual behavior after opening the door reinforced the  
5 officers' reasonable suspicion that he would have run or disposed of the drugs if he had known  
6 police were closing in. Id. The Court found that the magistrate's initial rejection of a no-knock  
7 warrant did "not alter the reasonableness of the officers' decision" to proceed without knocking  
8 and announcing, "which must be evaluated as of the time they entered the motel room." Id. The  
9 Court reasoned that the issuing magistrate could not know of the actual circumstances the  
10 officers' would encounter when he denied the agents' request for a special warrant. Id. at  
11 395-96. As such, "a magistrate's decision not to authorize a no-knock entry should not be  
12 interpreted to remove the officers' authority to exercise independent judgment concerning the  
13 wisdom of a no-knock entry at the time the warrant is being executed." Id. at 396 n.7.

14 Here, too, the United States' actions were reasonable. The investigative agents filed a  
15 return two days after the execution of the search warrant detailing the devices seized from the  
16 premises, and within approximately 30 days after the execution of the warrant Agent Daun  
17 destroyed any forensic images of devices that did not contain material responsive to the search  
18 warrant. The physical devices that did not contain responsive material or contraband have been  
19 segregated for return to defendant and have not been searched.

20 On the same day the search warrant was executed, Agent Daun found a file labeled  
21 "filesalot.dcv" that contains the bulk of the incriminating information in this case. Due to the  
22 volume of data involved, Agent Daun spent considerable time identifying particular files and  
23 pieces of data within files that the search warrant commands law enforcement to seize. The  
24 images that Agent Daun continues to review were all promptly determined to contain evidence  
25 or contraband, and the scope of the search has not expanded beyond the contours of the search  
26 warrant. Defendant cites no case for the remarkable proposition that law enforcement can no  
27 longer look at evidence of crime once it has been properly seized. Such a rule would be wholly  
28

1 impractical and entirely inconsistent with how physical evidence is handled. See, e.g., United  
2 States v. Prime, 431 F.3d 1147, 1151 (9th Cir. 2004) (admitting testimony regarding handwriting  
3 analysis of documents used in crime); United States v. Sherwood, 98 F.3d 402, 408 (9th Cir.  
4 1996) (admitting testimony regarding fingerprint analysis of parking ticket). Here, the length  
5 of time that the United States has spent analyzing the lawfully seized material is reasonable in  
6 light of the amount of incriminating data seized and the defendant's efforts at concealing his  
7 crimes through encryption, false identities, and other methods. Similarly, defendant provides  
8 no authority to support his motion to order the United States to digitally and then physically  
9 destroy the devices and forensic images lawfully seized as evidence pursuant to search warrant.  
10 See Mot. Order Re Data Deletion (CR 847) at 6-7.

11 **III. Conclusion.**

12 As argued above, the United States' collection of historical records pursuant to subpoenas  
13 and court orders was reasonable, the FBI's efforts to locate the Aircard pursuant to Warrant CR-  
14 08-90330 were reasonable, and the searches of defendant's apartment and computers pursuant  
15 to the search warrant were reasonable. Moreover, under all of the facts and circumstances of this  
16 case, defendant, a person with no known lawful source of income, had no reasonable expectation  
17 of privacy in the Aircard and Aircard account he purchased and maintained through the  
18 fraudulent assumption of another living person's identity. Accordingly, defendant's motion to  
19 suppress and all related motions should be denied.

20 Respectfully submitted this 20<sup>th</sup> day of August, 2012.

21 JOHN S. LEONARDO  
22 United States Attorney  
District of Arizona

23 S/Frederick A. Battista  
24 FREDERICK A. BATTISTA

25 S/James R. Knapp  
26 JAMES R. KNAPP

27 PETER S. SEXTON  
28 Assistant U.S. Attorneys

**Certificate of Service**

I hereby certify that on August 20, 2012, I filed the attached document via electronic transmission to the Clerk's Office using the CM/ECF system for filing and transmittal of a Notice of Electronic Filing to the following CM/ECF registrant:

Phil Seplow  
Shadow Counsel for Defendant

On August 21, 2012, copy of the attached document will also be mailed to:

Daniel David Rigmaiden  
Agency No. 10966111  
CCA-CADC  
PO Box 6300  
Florence, AZ 85132

S/James R. Knapp

JAMES R. KNAPP  
Assistant U.S. Attorney